SMART DUMM

Was dein Smartphone über dich weiß
(und was du besser wissen solltest)



Über mich

Ich wurde 1969 geboren und bin seit 1982 ein begeisterter Fan von Computern. Angefangen hat alles mit meinem ersten eigenen Gerät – einem Commodore VIC-20. Danach folgten der legendäre C64, die faszinierenden Amiga-Computer und später Systeme mit Windows, macOS und Linux. Technik hat mich von Anfang an fasziniert – egal ob 8-Bit-Klassiker oder moderne Hochleistungsrechner.



Beruflich habe ich viele Bereiche der IT erlebt: Ich war Netzwerkadministrator, IT-Supporter, Webdesigner, Qualitätsprüfer in der IT-Branche und IT-Administrator. Über die Jahre konnte ich in vielen Rollen erleben, wie sich die digitale Welt immer weiterentwickelt hat – und diese Erfahrung prägt bis heute meinen Blick auf Technologie.

Neben meiner Arbeit bin ich Sammler und Liebhaber alter Computer aus der 8- und 16-Bit-Zeit. Die Geräte dieser Ära sind für mich nicht nur Technik, sondern echte Zeitzeugen voller Charakter. Gleichzeitig begeistert mich die Welt der Smartphones – von Android bis iOS – und die rasante Entwicklung mobiler Technologien.

Mit diesem Buch möchte ich mein Wissen und meine Leidenschaft weitergeben – verständlich, praxisnah und immer mit einem kleinen Augenzwinkern. **BTW**: Das Bild und das Cover stammen von ChatGPT, mit mir als Vorlage und ein wenig Magic von dem Malprogramm GIMP.

Einleitung

Willkommen zu diesem Buch – einem etwas anderen Blick auf unser alltägliches, aber oft unterschätztes Gerät: das Smartphone. Ob du schon lange mit deinem Handy vertraut bist oder gerade erst anfängst, dich intensiver damit zu beschäftigen – dieses Buch ist für alle, die mehr wollen als nur Tippen, Wischen und Selfies.

Hier geht es nicht nur um Technik, sondern auch um Verständnis, Hintergründe und vor allem: Sicherheit. In einer Welt, in der das Smartphone mehr über uns weiß als so mancher Mensch, lohnt sich ein genauer Blick auf das, was in unserer Hosentasche schlummert – und was es über uns verrät.

Dieses Buch ist sicherlich nicht das komplexeste Werk über Smartphones und digitale Sicherheit – und das ist auch gut so. Denn es will nicht verwirren, sondern verständlich machen. Es ist geschrieben für alle: für Neugierige, für Skeptiker, für Technikinteressierte – und für alle, die ein bisschen mehr wissen wollen, ohne Informatik studieren zu müssen.

Ein Dank geht an alle Freunde und Bekannte, die das Buch hier einmal quer gelesen haben. Eure Tipps und Anmerkungen waren sehr wertvoll!

Also: Mach dein Handy lautlos, lehn dich zurück – und entdecke, was du bisher vielleicht übersehen hast.

Von der Wählscheibe zum digitalen Alleskönner

Die Geschichte des Telefons bis zum Smartphone

Die Geschichte des Telefons beginnt mit einem Paukenschlag im Jahr 1876, als Alexander Graham Bell das erste funktionsfähige Telefon patentieren ließ. Seine Erfindung war eine Sensation: Zum ersten Mal konnte Sprache über elektrische Leitungen übertragen werden – eine Revolution in der Kommunikation. Die ersten Geräte waren sperrig, bestanden aus Holz, Kabeln und Metallteilen und wurden meist fest an einer Wand montiert. Telefonieren war ein echtes Event, meist mit Vermittlungsstellen dazwischen, in denen Menschen noch per Hand Verbindungen herstellten.

In den folgenden Jahrzehnten entwickelte sich das Telefon weiter – sowohl technisch als auch gesellschaftlich. Ab den 1920er-Jahren wurde das Drehscheibentelefon populär, bei dem jede Ziffer mühsam „gedreht" wurde. Es folgten Tastenfelder in den 1960ern, die das Wählen deutlich beschleunigten. Aber bis weit ins 20. Jahrhundert hinein war das Telefon fest mit einem Ort verbunden: dem Wohnzimmer, dem Flur oder dem Büro.

Die große Befreiung kam in den 1980er-Jahren mit dem Mobiltelefon. Die ersten sogenannten „Mobiltelefone" waren allerdings alles andere als handlich – groß, schwer und mit begrenzter Akkulaufzeit. Das wohl bekannteste Modell dieser Zeit war das Motorola DynaTAC 8000X, das 1983 erschien. Es wog fast ein Kilo, bot 30 Minuten Gesprächszeit und kostete über 3.000 Dollar – ein Statussymbol der Extraklasse.

In den 1990ern begann der Siegeszug der handlichen Mobiltelefone. Geräte wie das Nokia 3310 wurden millionenfach verkauft und prägten eine Generation. SMS-Nachrichten, polyphone Klingeltöne und vorinstallierte Spiele wie „Snake“ machten die Geräte zu mehr als nur Telefonen – sie wurden zu persönlichen Begleitern.

Der nächste große Umbruch kam mit dem Aufstieg des Smartphones. Während erste Smartphone-ähnliche Geräte wie der IBM Simon (1994) oder später Blackberrys bereits einige smarte Funktionen boten, war es das iPhone von Apple im Jahr 2007, das die mobile Welt grundlegend veränderte. Der kapazitive Touchscreen, der vollständig auf physische Tasten verzichtete, die intuitive Benutzeroberfläche und die Möglichkeit, Apps zu installieren, machten das Smartphone zum universellen Werkzeug des digitalen Zeitalters.

Seitdem hat sich das Smartphone zum multifunktionalen Alleskönner entwickelt. Es vereint Telefon, Kamera, Navigationsgerät, Taschenrechner, Kalender, Internetzugang, Spielekonsole, Musikplayer und vieles mehr in einem einzigen kompakten Gerät. Mit dem Aufkommen von mobilem Internet, 4G, 5G und cloudbasierten Diensten ist das Smartphone heute das Zentrum unseres digitalen Lebens.

Während das Telefon einst ein Gerät war, mit dem man gezielt einen anderen Menschen kontaktierte, ist das Smartphone heute eine permanente Verbindung zur Welt. Es informiert, unterhält, organisiert und überwacht – und ja, telefonieren kann es auch noch.

Empfehlenswerte Quellen

Wikipedia: Geschichte des Telefons
https://de.wikipedia.org/wiki/Geschichte_des_Telefons

Wikipedia: Smartphone
https://de.wikipedia.org/wiki/Smartphone

The Smithsonian Goes Telephonic in 1878!
https://siarchives.si.edu/blog/smithsonian-goes-telephonic-1878

Motorola DynaTAC 8000X – Das erste Mobiltelefon
https://en.wikipedia.org/wiki/Motorola_DynaTAC

IBM Simon – Das erste Smartphone
https://en.wikipedia.org/wiki/IBM_Simon

Das Smartphone kurz vorgestellt

Was steckt eigentlich in einem Smartphone?
Ein Blick unter die Haube

Man trägt es ständig bei sich, behandelt es besser als so manchen Mitmenschen und gerät in Panik, wenn der Akkustand unter 10 % fällt: das Smartphone. Aber was steckt eigentlich drin in diesem kleinen Zauberkästchen, das uns täglich durch den Alltag begleitet?

1. Das Gehirn: Der Prozessor (aka SoC)

Im Zentrum jedes Smartphones werkelt der Prozessor – quasi das Hirn des Ganzen. Heute ist das meist ein sogenanntes System-on-a-Chip (SoC), das nicht nur denkt, sondern auch gleich für Grafik, Speicher und sogar Funk zuständig ist. Ein echtes Multitalent! Wäre es ein Mensch, hätte es fünf Jobs, nie Urlaub – und trotzdem keine Beschwerden.

2. Speicher – das Gedächtnis des Geräts

Hier gibt's zwei Sorten: RAM (Arbeitsspeicher) – das Kurzzeitgedächtnis, wo Apps zwischengelagert werden – und den internen Speicher, wo alles Wichtige dauerhaft wohnt: Urlaubsfotos, Chatverläufe und 37 Versionen derselben To-do-Liste.

3. Das Display – unser Fenster zur digitalen Welt

Das Display ist das Gesicht des Smartphones. Es zeigt uns alles – von Katzenvideos bis zur Wetterwarnung. Und weil wir es nonstop antatschen, ist es gleichzeitig auch die Steuerzentrale. Moderne Displays (meist OLED oder LCD) sind so scharf, dass du jedes Pixel deiner Selfies bewundern kannst – oder fürchtest.

4. Kameras – und zwar viele davon

Heutzutage hat ein Smartphone oft mehr Kameras als ein Fotograf Ausrüstung. Hauptkamera, Weitwinkel, Makro, Selfiecam – jedes Objektiv hat seine Aufgabe. Und alle zusammen sind dafür da, dass du dein Mittagessen endlich in 4K mit der Welt teilen kannst.

5. Sensoren – die heimlichen Helfer

Diese kleinen Spione merken, wann du dein Handy drehst, ob du es ans Ohr hältst oder wie schnell du rennst (oder eher gehst). Vom Fingerabdrucksensor über den Lichtsensor bis zum digitalen Kompass – dein Smartphone weiß oft mehr über dich als dein bester Freund.

6. Verbindungen – Hauptsache erreichbar

Damit du jederzeit TikToks schauen, Pizza bestellen oder dich (versehentlich) im Internet verirren kannst, hat dein Smartphone WLAN, Bluetooth, GPS, 4G, 5G – und manchmal sogar noch Gefühl für Humor, wenn der Empfang genau dann weg ist, wenn du ihn brauchst.

7. Akku – der Treibstoff des Alltags

Ohne Akku läuft nix. Meist ein Lithium-Ionen-Kraftwerk, das alles mit Energie versorgt – bis du TikTok öffnest, dann ist der Akku plötzlich durstig wie ein Kamel in der Wüste. Geladen wird per USB-C oder, wenn du Apple nutzt, per Lightning-Kabel aus der Zukunft.

8. Gehäuse – Schick und stabil (meistens)

Die Hülle schützt die empfindliche Technik. Mal aus Plastik, mal aus Glas oder Metall – je nachdem, wie sehr du dein Handy bei einem Sturz weinen hören willst. Tipp: Hüllen helfen. Meistens.

Empfehlenswerte Quellen

Wikipedia: Smartphone
https://de.wikipedia.org/wiki/Smartphone

Wikipedia: System-on-a-Chip (SoC)
https://de.wikipedia.org/wiki/System-on-a-Chip

ARM-Architektur und Prozessoren (offizielle ARM Webseite)
https://www.arm.com/architecture

Heise Online: „Was steckt alles in einem Smartphone?"
https://www.heise.de/bestenlisten/ratgeber/welche-komponenten-stecken-in-einem-aktuellen-smartphone/s64978n

Heise Online: Welche Sensoren hat ein Smartphone?
https://www.heise.de/tipps-tricks/Welche-Sensoren-hat-ein-Smartphone-6603628.html

Anatomy of a smartphone launch
https://www.androidauthority.com/anatomy-smartphone-launch-566388/

Drei Computer in deiner Hosentasche

Das Smartphone-Trio

Du denkst, dein Smartphone ist nur ein Gerät? Falsch gedacht! In Wirklichkeit beherbergt es ein Trio von Computern, die gemeinsam dafür sorgen, dass du jederzeit erreichbar bist, Selfies schießen und Katzenvideos streamen kannst. Lernen wir die drei mal kennen:

1. Der SIM-Karten-Computer – dein digitaler Ausweis

Die SIM-Karte (Subscriber Identity Module) ist nicht nur ein kleiner Chip, sondern ein vollwertiger Computer im Mini-Format. Sie speichert deine Identität im Mobilfunknetz, inklusive deiner Telefonnummer und Zugangsdaten. Ohne sie wüsste dein Smartphone nicht, wer du bist – und das Netz auch nicht. Sie ist quasi dein digitaler Ausweis, der dich im Netzwerk authentifiziert und dafür sorgt, dass du telefonieren und surfen kannst.

2. Der Telefon-Computer – die Kommunikationszentrale

Der zweite Computer ist das eigentliche Herzstück deines Smartphones: der Prozessor, auch bekannt als System-on-a-Chip (SoC). Er verarbeitet alle deine Eingaben, steuert das Betriebssystem, führt Apps aus und sorgt dafür, dass alles reibungslos läuft. Ohne ihn wäre dein Smartphone nur ein teurer Briefbeschwerer.

3. Der Verbindungs-Computer – der Netzwerker

Der dritte im Bunde ist der Kommunikationsprofi. Er sorgt dafür, dass dein Smartphone mit der Außenwelt verbunden ist – sei es über Mobilfunk, WLAN, Bluetooth oder GPS. Er koordiniert die Datenströme, hält dich online und ermöglicht es dir, in Echtzeit mit Freunden zu chatten oder den Weg zum nächsten Café zu finden.

Fazit - Mehr als nur ein Telefon! Dein Smartphone ist also nicht nur ein Gerät, sondern ein Team aus drei spezialisierten Computern, die Hand in Hand arbeiten, um dir das Leben zu erleichtern. Also, beim nächsten Mal, wenn du dein Smartphone benutzt, denk daran: Du hast ein echtes Technik-Trio in der Tasche!

Empfehlenswerte Quellen

Wikipedia: Subscriber Identity Module (SIM-Karte)
https://de.wikipedia.org/wiki/Simkarte

Wikipedia: System-on-a-Chip (SoC)
https://de.wikipedia.org/wiki/System-on-a-Chip

Wikipedia: WLAN
https://de.wikipedia.org/wiki/Wireless_Local_Area_Network

Kommunikationstechnologien in Smartphones
https://digitale-identitaeten.de/digitale-identitaeten-das-kleine-1x1-der-sicheren-digitalen-identitaeten/

Die SIM-Karte

Klein, klug, unterschätzt (und bald unsichtbar)

Sie ist winzig, sieht aus wie ein Stück technischer Knabberkram und kommt auch mal mit der Post – die SIM-Karte. Doch unterschätz sie nicht! Dieses kleine Wunderwerk ist der Türsteher deines digitalen Ichs. Ohne sie? Kein Netz, keine Anrufe, kein "Ich schreib dir bei WhatsApp". Nur du und ein extrem teures Stück Glas und Metall, das bestenfalls noch die Uhr anzeigen kann.

SIM steht für „Subscriber Identity Module". Klingt hochtrabend, aber im Grunde macht sie genau das: Sie weiß, wer du bist – zumindest aus Sicht deines Mobilfunkanbieters. Deine Telefonnummer, Zugangsdaten, Netzwerkeinstellungen – alles gespeichert auf einem kleinen Chip, der kaum größer ist als ein Fingernagel.

Und das Beste: Die SIM ist ein eigenständiger Mini-Computer! Sie besitzt ihren eigenen Prozessor, ein Betriebssystem im ROM und – ja, wirklich – RAM. Zugegeben, mit 8 bis 128 Kilobyte nicht gerade ein Kraftpaket, aber hey, für ein bisschen Identität reicht's. Sie speichert Kontakte, ein paar SMS und kann sogar kleine Programme ausführen, dank des sogenannten SIM Application Toolkits. Also: ein Chip mit Charakter!

Im Laufe der Jahre hat die gute alte SIM übrigens eine beachtliche Diät hingelegt. Von der Scheckkartengröße über Mini, Micro und Nano ist sie mittlerweile so klein, dass du sie nur noch mit spitzen Fingern einsetzen kannst – und selbst dabei die Nerven verlierst.

Und jetzt kommt die eSIM.

Die “embedded SIM” (also: fest eingebaute SIM) ist wie die SIM-Karte – nur ohne Karte. Sie ist direkt im Smartphone verbaut und wird digital vom Anbieter aktiviert. Du musst also nichts mehr fummeln, nichts mehr zuschneiden (ja, manche haben das echt mit der Nagelschere gemacht!) und kannst theoretisch in Sekunden den Anbieter wechseln – zumindest, wenn dein Vertrag das auch so sieht.

Die eSIM ist praktisch, sicherer und zukunftsfreundlich – aber irgendwie auch ein bisschen unromantisch. Kein Gefummel mehr mit Büroklammern, kein panisches „Wo ist meine SIM-Karte?!“ nach dem Wechsel aufs neue Handy. Dafür aber pure Effizienz.

Fazit - Ob klassische SIM oder moderne eSIM – ohne diese kleinen digitalen Genies wär dein Smartphone nur ein netter Spiegel mit Kamera. Also verneige dich ruhig mal vor dem stillen Helden im Inneren. Oder dem gar nicht mehr sichtbaren.

Empfehlenswerte Quellen

Wikipedia: SIM-Karte
https://de.wikipedia.org/wiki/SIM-Karte

Wikipedia: eSIM
https://de.wikipedia.org/wiki/ESIM

GSMA (Global System for Mobile Communications Association): Was ist eine eSIM?
https://www.gsma.com/esim/

Nano-, Micro- und eSIM – die Simkarten-Größen im Überblick
https://inside-sim.de/4523/nano-micro-und-esim-die-simkarten-groessen-im-ueberblick/

eSIM – was ist das? Kurz und einfach erklärt
https://esim.holafly.com/de/esim-karte/was-ist-eine-esim

Vom Rechenknecht zum Taschenzauberer

Die Geschichte der Smartphone-Prozessoren

In den Anfängen der Computerära dominierten große, stromhungrige Prozessoren die Szene. Mit der Zeit wurden sie kleiner, effizienter und fanden schließlich ihren Weg in unsere Hosentaschen – als Herzstück unserer Smartphones.

Die meisten modernen Smartphones nutzen Prozessoren, die auf der ARM-Architektur basieren. ARM, ursprünglich von der britischen Firma Acorn entwickelt, zeichnet sich durch eine energieeffiziente und skalierbare Architektur aus. Diese Eigenschaften machen ARM-Prozessoren ideal für mobile Geräte, die auf lange Akkulaufzeiten angewiesen sind. Hersteller wie Qualcomm mit ihrer Snapdragon-Serie oder Samsung mit den Exynos-Chips setzen auf ARM-Designs, um leistungsstarke und gleichzeitig stromsparende Prozessoren zu entwickeln.

Ein Grund, warum Apps von PCs nicht direkt auf Smartphones laufen, liegt in der unterschiedlichen Prozessorarchitektur. Während PCs meist auf der x86-Architektur basieren, nutzen Smartphones ARM-Architekturen. Diese Unterschiede führen dazu, dass Software speziell für die jeweilige Architektur entwickelt oder angepasst werden muss. Zwar gibt es Emulatoren und Übersetzer, die eine gewisse Kompatibilität ermöglichen, doch sind diese Lösungen oft mit Leistungseinbußen verbunden.

Interessanterweise verschwimmen die Grenzen zwischen den Architekturen zunehmend. Apple hat beispielsweise begonnen, seine

Macs mit ARM-basierten Prozessoren auszustatten, was eine Annäherung der beiden Welten bedeutet.

Insgesamt zeigt die Entwicklung der Smartphone-Prozessoren, wie technologische Innovationen unsere täglichen Begleiter leistungsfähiger und effizienter gemacht haben – und das alles in einem Gerät, das bequem in unsere Tasche passt.

Empfehlenswerte Quellen

Wikipedia: ARM-Architektur
https://de.wikipedia.org/wiki/ARM-Architektur

Wikipedia: System-on-a-Chip (SoC)
https://de.wikipedia.org/wiki/System-on-a-Chip

ARM Ltd. – Offizielle Webseite: Über ARM und seine Technologie
https://www.arm.com/architecture

ARM vs x86: Wird Apple Intel und AMD in CPUs dominieren?
https://itigic.com/de/arm-vs-x86-will-apple-dominate-intel-and-amd-in-cpus/

Smartphone-Prozessoren: Große Unterschiede bei SoCs
https://www.inside-digital.de/ratgeber/smartphone-prozessoren-diese-unterschiede-bei-socs-musst-du-kennen

Apple Pressemitteilung: Einführung der M1-Chips (ARM-basierte Macs)
https://www.apple.com/newsroom/2020/11/apple-unleashes-m1/

Die Evolution der mobilen Betriebssysteme

Von der Wählscheibe zum Touchscreen

1. Die Anfänge: Symbian und Palm OS

Symbian OS war einst der unangefochtene König der mobilen Betriebssysteme. Ursprünglich aus dem EPOC-System von Psion hervorgegangen, wurde es in den späten 1990er- und frühen 2000er-Jahren von Nokia und anderen Herstellern wie Sony Ericsson und Motorola genutzt. Symbian war bekannt für seine Energieeffizienz und Anpassungsfähigkeit, aber seine Benutzeroberfläche galt als wenig intuitiv. Mit dem Aufkommen von iOS und Android verlor Symbian schnell an Bedeutung und wurde 2012 offiziell eingestellt.

Palm OS, auch bekannt als Garnet OS, wurde 1996 von Palm, Inc. für PDAs entwickelt. Es war eines der ersten Betriebssysteme mit einer benutzerfreundlichen Touchscreen-Oberfläche und bot grundlegende Anwendungen wie Kalender, Adressbuch und Notizen. Palm OS war besonders in den USA beliebt, verlor jedoch mit dem Aufkommen moderner Smartphones an Relevanz und wurde 2009 eingestellt.

2. Die Ära der Smartphones: BlackBerry OS und Windows Mobile

BlackBerry OS wurde von Research In Motion (RIM) entwickelt und war besonders bei Geschäftsleuten beliebt, dank seiner physischen Tastatur und sicheren E-Mail-Funktionen. Trotz seiner frühen Erfolge konnte BlackBerry OS nicht mit den Innovationen von iOS und Android Schritt halten und wurde schließlich eingestellt.

Windows Mobile war Microsofts Versuch, den mobilen Markt zu erobern. Es bot eine vertraute Benutzeroberfläche für Windows-Nutzer,

litt jedoch unter mangelnder App-Unterstützung und einer weniger benutzerfreundlichen Oberfläche. Microsoft stellte Windows Mobile zugunsten von Windows Phone ein, das ebenfalls keinen langfristigen Erfolg hatte.

3. Die Giganten: iOS und Android

iOS, entwickelt von Apple, wurde 2007 mit dem ersten iPhone eingeführt. Es zeichnete sich durch eine intuitive Benutzeroberfläche, regelmäßige Updates und ein umfangreiches App-Ökosystem aus. iOS bleibt exklusiv für Apple-Geräte und hat sich über die Jahre kontinuierlich weiterentwickelt, zuletzt mit iOS 17, das Funktionen wie interaktive Widgets und verbesserte Datenschutzoptionen bietet.

Android, ein Open-Source-Betriebssystem basierend auf dem Linux-Kernel, wurde 2008 von Google eingeführt. Es bietet Herstellern die Flexibilität, eigene Benutzeroberflächen zu erstellen, was zu einer Vielzahl von Geräten mit unterschiedlichen Funktionen führte. Android hat sich schnell zum weltweit meistgenutzten mobilen Betriebssystem entwickelt, mit der neuesten Version Android 15, die Verbesserungen in Datenschutz und KI-Integration bietet.

4. Alternative Ansätze: Firefox OS, HarmonyOS und HyperOS

Firefox OS, entwickelt von Mozilla, war ein Open-Source-Betriebssystem, das vollständig auf Webtechnologien basierte. Trotz seines innovativen Ansatzes konnte es sich nicht auf dem Markt durchsetzen und wurde 2017 eingestellt.

HarmonyOS, entwickelt von Huawei, wurde als Reaktion auf US-Sanktionen eingeführt, die den Zugang zu Android einschränkten. Es ist ein mikrokernelbasiertes, verteiltes Betriebssystem, das für verschiedene Gerätetypen entwickelt wurde. In China hat HarmonyOS bereits einen bedeutenden Marktanteil erreicht und wird kontinuierlich weiterentwickelt.

Xiaomi HyperOS ist Xiaomis neuer Ansatz, um ein einheitliches Betriebssystem für Smartphones, IoT-Geräte und sogar Fahrzeuge zu schaffen. Es basiert auf Android und NuttX und ersetzt das bisherige MIUI. HyperOS wurde 2023 eingeführt und zielt darauf ab, ein nahtloses Benutzererlebnis über verschiedene Gerätetypen hinweg zu bieten.

Fazit - Die Welt der mobilen Betriebssysteme hat eine beeindruckende Entwicklung durchlaufen – von den frühen Tagen der Wählscheiben-Telefone bis hin zu den heutigen Smartphones, die mehr Rechenleistung besitzen als die Computer, die einst Menschen zum Mond brachten. Während einige Systeme wie Symbian und Palm OS heute nur noch in den Geschichtsbüchern zu finden sind, dominieren iOS und Android den aktuellen Markt. Gleichzeitig zeigen neue Entwicklungen wie HarmonyOS und HyperOS, dass Innovation und Wettbewerb weiterhin lebendig sind – und wer weiß, vielleicht steht das nächste große Betriebssystem bereits in den Startlöchern.

Empfehlenswerte Quellen

Wikipedia: Symbian
https://de.wikipedia.org/wiki/Symbian

Wikipedia: Palm OS
https://de.wikipedia.org/wiki/Palm_OS

Wikipedia: BlackBerry OS
https://de.wikipedia.org/wiki/BlackBerry_OS

Wikipedia: Windows Mobile
https://de.wikipedia.org/wiki/Windows_Mobile

Wikipedia: iOS
https://de.wikipedia.org/wiki/IOS

Wikipedia: Android (Betriebssystem)
https://de.wikipedia.org/wiki/Android_(Betriebssystem)

Wikipedia: Firefox OS
https://de.wikipedia.org/wiki/Firefox_OS

Wikipedia: HarmonyOS
https://de.wikipedia.org/wiki/HarmonyOS

Xiaomi HyperOS (aktuell nur auf englisch detailliert dokumentiert)
https://www.mi.com/global/hyperos/

Was ist WLAN?

WLAN steht für Wireless Local Area Network, also ein drahtloses lokales Netzwerk. Es ermöglicht die Verbindung von Geräten wie Smartphones, Laptops oder Tablets mit dem Internet oder untereinander, ohne dass Kabel erforderlich sind.

Ursprung und Entwicklung

Die Anfänge der WLAN-Technologie reichen bis in die 1970er Jahre zurück. Ein bedeutender Meilenstein war die Entwicklung von ALOHAnet an der University of Hawaii, das 1971 als erstes drahtloses Computernetzwerk in Betrieb genommen wurde.

In den 1990er Jahren wurde die WLAN-Technologie weiterentwickelt. 1991 entwickelten die Unternehmen NCR Corporation und AT&T in Nieuwegein, Niederlande, das WaveLAN, ein Vorläufer des heutigen WLANs.

1997 veröffentlichte das Institute of Electrical and Electronics Engineers (IEEE) den ersten WLAN-Standard unter dem Namen IEEE 802.11, der Datenübertragungsraten von bis zu 2 Mbit/s ermöglichte. Zwei Jahre später, 1999, folgte der Standard 802.11b, der Geschwindigkeiten von bis zu 11 Mbit/s bot.

Wi-Fi und die Wi-Fi Alliance

Der Begriff Wi-Fi wurde 1999 von der Markenberatungsfirma Interbrand im Auftrag der Wi-Fi Alliance eingeführt. Er ist ein Kunstwort, das als Anspielung auf “Hi-Fi” (High Fidelity) gedacht war und sollte einen eingängigeren Namen als “IEEE 802.11b” bieten. Die Wi-Fi Alliance ist ein Zusammenschluss von Unternehmen, der Geräte

zertifiziert, die den IEEE-802.11-Standards entsprechen, um die Interoperabilität zwischen verschiedenen Herstellern zu gewährleisten.

Verbreitung und Bedeutung

Heute ist WLAN aus dem Alltag nicht mehr wegzudenken. Es ermöglicht den drahtlosen Internetzugang in Haushalten, Unternehmen, öffentlichen Einrichtungen und an vielen öffentlichen Orten wie Cafés, Flughäfen und Bahnhöfen. Die Technologie hat sich stetig weiterentwickelt, mit neuen Standards wie 802.11n, 802.11ac und 802.11ax (Wi-Fi 6), die höhere Geschwindigkeiten und bessere Leistung bieten.

In Deutschland und weltweit ist WLAN ein zentraler Bestandteil der digitalen Infrastruktur und spielt eine entscheidende Rolle in der modernen Kommunikation und Informationstechnologie.

WLAN, Smartphones und VPNs: Ein Blick auf die digitale Sicherheit

In der heutigen digitalen Welt ist es kaum vorstellbar, ohne WLAN und Smartphones auszukommen. Doch während wir uns bequem mit Netzwerken verbinden, lauern im Hintergrund potenzielle Gefahren. Ein VPN (Virtual Private Network) kann dabei helfen, unsere Daten zu schützen und unsere Privatsphäre zu wahren.

Wie verbindet sich ein Smartphone mit einem WLAN?

Wenn ein Smartphone ein bekanntes WLAN-Netzwerk erkennt, sendet es automatisch eine Anfrage zur Verbindung. Dabei werden Informationen wie die SSID (Netzwerkname) und die MAC-Adresse des Geräts ausgetauscht. Sobald die Verbindung hergestellt ist, beginnt der Datenverkehr zwischen dem Smartphone und dem Router.

Wie können Smartphones über WLAN verfolgt werden?

Jedes Mal, wenn ein Smartphone nach verfügbaren Netzwerken sucht, sendet es sogenannte “Probe Requests” aus. Diese Anfragen enthalten unverschlüsselt die MAC-Adresse des Geräts, die als eindeutiger Identifikator dient und auch andere Daten, wie zum Beispiel die Namen der WLANs mit denen du schon einmal verbunden warst. So eine „Anfrage“ ist wie ein Ruf nach „Bin ich zu Hause? Bist mein WLAN?“. Öffentliche WLAN-Netzwerke oder böswillige Akteure können diese Informationen nutzen, oder zum Beispiel der Supermarkt von nebenan erkennt dich schon vor dem Eingang und sendet dir die schönsten Angebote.

Warum ist ein VPN in öffentlichen WLANs sinnvoll?

Öffentliche WLANs, wie sie in Cafés oder Flughäfen angeboten werden, sind oft ungesichert. Cyberkriminelle können diese Netzwerke nutzen, um Daten abzufangen oder gefälschte Zugangspunkte (sogenannte “Evil Twins”) zu erstellen. Ein VPN verschlüsselt den gesamten Datenverkehr zwischen dem Smartphone und dem Internet, wodurch es für Dritte nahezu unmöglich wird, sensible Informationen auszuspähen.

Fazit - Während WLAN und Smartphones unseren Alltag erleichtern, ist es wichtig, sich der potenziellen Risiken bewusst zu sein. Ein VPN bietet eine zusätzliche Sicherheitsebene, insbesondere in öffentlichen Netzwerken, und hilft dabei, unsere digitalen Spuren zu verwischen. Denn in der digitalen Welt gilt: Vorsicht ist besser als Nachsicht.

Empfehlenswerte Quellen

Wikipedia: WLAN
https://de.wikipedia.org/wiki/Wireless_Local_Area_Network

Wikipedia: IEEE 802.11
https://de.wikipedia.org/wiki/IEEE_802.11

Wikipedia: ALOHAnet
https://en.wikipedia.org/wiki/ALOHAnet

Wi-Fi Alliance – Offizielle Webseite
https://www.wi-fi.org/

WLAN Standards - die Unterschiede im Überblick
https://praxistipps.chip.de/wlan-standards-die-unterschiede-im-ueberblick_31063

Golem.de: Wireless LAN
https://www.golem.de/specials/wlan/

WiFi Probe Requests Explained
https://blog.spacehuhn.com/probe-request

Was ist ein VPN?

Ein VPN ist wie ein magischer Umhang, der Ihre Online-Aktivitäten vor neugierigen Blicken schützt. Es erstellt einen sicheren, verschlüsselten Tunnel zwischen Ihrem Gerät und dem Internet. So können Sie sicher surfen, selbst wenn Sie sich in einem öffentlichen WLAN befinden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt es als eine Möglichkeit, Daten über unsichere Netzwerke sicher zu übertragen, indem der Datenverkehr innerhalb des VPNs verschlüsselt wird .

Wie funktioniert ein VPN?

Wenn Sie ein VPN aktivieren, passiert Folgendes:

- Ihr Gerät stellt eine Verbindung zu einem VPN-Server her.
- Alle Daten, die Sie senden oder empfangen, werden durch einen verschlüsselten Tunnel geleitet.
- Ihre IP-Adresse wird durch die des VPN-Servers ersetzt, wodurch Ihre Identität und Ihr Standort verborgen bleiben.

Laut Wikipedia ermöglicht ein VPN eine Netzwerkverbindung, die von Unbeteiligten nicht einsehbar ist, indem es Daten verschlüsselt und die IP-Adresse des Nutzers verbirgt.

Warum ist ein VPN wichtig?

In öffentlichen WLANs, wie in Cafés oder Flughäfen, sind Ihre Daten besonders gefährdet. Cyberkriminelle können leicht auf ungesicherte Verbindungen zugreifen und persönliche Informationen stehlen. Ein VPN schützt Sie, indem es Ihre Daten verschlüsselt und Ihre Identität verbirgt. Das BSI empfiehlt die Nutzung von VPNs, um die Privatsphäre

im Internet zu erhöhen und sich vor Zugriffen aus dem restlichen Internet zu schützen.

Weitere Vorteile eines VPNs

Zugriff auf gesperrte Inhalte: Ein VPN kann Ihnen helfen, geografische Beschränkungen zu umgehen und auf Inhalte zuzugreifen, die in Ihrem Land nicht verfügbar sind.

Sicheres Arbeiten von überall: Für Unternehmen ermöglicht ein VPN den sicheren Zugriff auf das Firmennetzwerk, egal wo sich die Mitarbeiter befinden.

Schutz vor Überwachung: Ein VPN schützt Sie vor neugierigen Blicken von Internetanbietern, Regierungen oder anderen Organisationen.

Die Wahl eines vertrauenswürdigen VPN-Anbieters ist entscheidend für Ihre Online-Sicherheit und Privatsphäre. Insbesondere bei Anbietern aus Ländern mit restriktiven Internetgesetzen oder fragwürdigen Datenschutzpraktiken können erhebliche Risiken bestehen.

Warum ist die Herkunft eines VPN-Anbieters wichtig?

VPNs sollen Ihre Daten schützen, indem sie Ihren Internetverkehr verschlüsseln und Ihre IP-Adresse verbergen. Doch nicht alle Anbieter garantieren diesen Schutz. In Ländern mit strenger Internetkontrolle und Überwachung, wie China und Russland, können VPN-Anbieter gesetzlich verpflichtet sein, Nutzerdaten an staatliche Stellen weiterzugeben oder bestimmte Inhalte zu blockieren.

Problematische VPN-Anbieter weltweit

Einige VPN-Dienste stehen im Verdacht, nicht ausreichend Datenschutz zu bieten oder sogar mit staatlichen Stellen zusammenzuarbeiten. Beispiele hierfür sind:

Hola VPN: Dieser Dienst wurde kritisiert, weil er die Bandbreite seiner Nutzer ohne deren Wissen an Dritte weiterverkauft hat, was erhebliche Sicherheitsrisiken birgt.

https://de.vpnmentor.com/reviews/hola-vpn/

HMA (ehemals HideMyAss!): Trotz der Behauptung, keine Logs zu speichern, hat HMA in der Vergangenheit Verbindungsdaten an Strafverfolgungsbehörden weitergegeben, was zur Identifizierung von Nutzern führte.

https://www.01net.com/de/vpn/hidemyass/

IPVanish: Obwohl der Anbieter eine No-Logs-Politik versprach, hat er in mindestens einem Fall detaillierte Verbindungsdaten an das FBI übermittelt.

https://www.computerbild.de/technik/vpn/tests/artikel/IPVanish-Was-kann-der-VPN-Dienst-aus-den-USA-24651692.html

Planet VPN: Dieser Dienst zeigt in seiner kostenlosen Version Werbung an und erlaubt Drittanbietern, umfangreiche Nutzerdaten für Werbezwecke zu sammeln, was die Privatsphäre der Nutzer gefährdet.

https://www.gutefrage.net/frage/ist-planet-vpn-sicher

Big Mama VPN: Dieser Anbieter verkauft die Internetverbindung seiner Nutzer an Dritte weiter, wodurch deren Geräte potenziell für Cyberkriminalität missbraucht werden können.

https://de.vpnmentor.com/reviews/bigmama-vpn/

Risiken bei der Nutzung solcher VPNs

Die Verwendung von VPNs mit fragwürdigen Datenschutzpraktiken kann folgende Gefahren mit sich bringen:

Datenweitergabe an Behörden: Anbieter könnten verpflichtet sein, Ihre Aktivitäten offenzulegen.

Eingeschränkte Funktionalität: Bestimmte Inhalte oder Dienste könnten blockiert sein.

Rechtliche Konsequenzen: In Ländern wie China kann die Nutzung nicht autorisierter VPNs zu Strafen führen.

Empfehlungen für vertrauenswürdige VPN-Anbiter

Um Ihre Privatsphäre zu schützen, sollten Sie VPNs wählen, die:

- Keine Logs speichern
- Sich in datenschutzfreundlichen Ländern befinden
- Transparente Geschäftsbedingungen haben

Beispiele für solche Anbieter sind:

ProtonVPN: Ansässig in der Schweiz, bekannt für strikte Datenschutzrichtlinien.

Mullvad VPN: Schwedischer Anbieter, der keine persönlichen Daten zur Anmeldung verlangt.

NordVPN: Mit Sitz in Panama, bietet starke Verschlüsselung und eine klare No-Logs-Politik.

Faustformeln für einen guten VPN Anbieter ist

- Ist der Anbieter zu günstig, dann lassen Sie die Finger davon.
- Ist der Anbieter aus einem Land mit Zensur (China, Russland, ect.), dann lassen Sie auch die Finger davon.
- Ein guter VPN Anbieter kommt am besten aus neutralen Ländern und verbirgt sich dazu, die Daten nicht weiter zu geben.

Lesen Sie erst alles Rechtliches von einem Anbieter und machen Sie sich selber schlau. Trauen Sie keiner Werbung. Suchen Sie nach Informationen zu dem VPN Anbieter im Internet. Meist reicht schon eine simple Wikipedia Suche.

VPN und die Länder

Ägypten

In Ägypten ist die Nutzung von VPN-Diensten nicht illegal, jedoch können sie zur Umgehung staatlicher Zensur eingesetzt werden, was problematisch sein kann. Das Anti-Cybercrime-Gesetz von 2018 erlaubt es der Regierung, Websites zu blockieren, die als Bedrohung für die nationale Sicherheit angesehen werden. Die Nutzung eines VPNs zum Zugriff auf solche Websites kann mit einer Freiheitsstrafe von bis zu einem Jahr oder einer Geldstrafe von bis zu 100.000 ägyptischen Pfund geahndet werden .

Einige VPN-Anbieter, die in Ägypten verfügbar sind:

ExpressVPN: Bietet schnelle Serververbindungen und eine benutzerfreundliche Oberfläche.

NordVPN: Bekannt für seine Sicherheitsfunktionen und eine große Anzahl an Servern weltweit.

Surfshark: Bietet unbegrenzte gleichzeitige Verbindungen und eine strikte No-Logs-Politik.

Es ist jedoch wichtig zu beachten, dass die ägyptische Regierung regelmäßig VPN-Dienste blockiert, was die Nutzung erschweren kann .

Bahrain

In Bahrain ist die Nutzung von VPN-Diensten legal, jedoch können sie zur Umgehung staatlicher Zensur eingesetzt werden, was problematisch sein kann. Die Regierung hat in der Vergangenheit Maßnahmen gegen die Nutzung von VPNs ergriffen, insbesondere wenn

sie zur Umgehung von Blockierungen von Websites oder sozialen Medien verwendet wurden.

Kuba

In Kuba ist die Nutzung von VPN-Diensten legal, jedoch unterliegt das Land strengen Internetkontrollen und Zensurmaßnahmen. Die Regierung hat in der Vergangenheit Maßnahmen gegen die Nutzung von VPNs ergriffen, insbesondere wenn sie zur Umgehung von Blockierungen von Websites oder sozialen Medien verwendet wurden.

Libyen

In Libyen ist die Nutzung von VPN-Diensten legal, jedoch unterliegt das Land strengen Internetkontrollen und Zensurmaßnahmen. Die Regierung hat in der Vergangenheit Maßnahmen gegen die Nutzung von VPNs ergriffen, insbesondere wenn sie zur Umgehung von Blockierungen von Websites oder sozialen Medien verwendet wurden.

Syrien

In Syrien ist die Nutzung von VPN-Diensten illegal. Die Regierung hat in der Vergangenheit Maßnahmen gegen die Nutzung von VPNs ergriffen, insbesondere wenn sie zur Umgehung von Blockierungen von Websites oder sozialen Medien verwendet wurden. Die Strafen für die Nutzung eines VPNs können schwerwiegende rechtliche Konsequenzen haben.

Vietnam

In Vietnam ist die Nutzung von VPN-Diensten legal, jedoch unterliegt das Land strengen Internetkontrollen und Zensurmaßnahmen. Die Regierung hat in der Vergangenheit Maßnahmen gegen die Nutzung von VPNs ergriffen, insbesondere wenn sie zur Umgehung von Blockierungen von Websites oder sozialen Medien verwendet wurden.

Russland

In Russland sind VPN-Dienste gesetzlich verpflichtet, mit den Behörden zusammenzuarbeiten und Nutzerdaten bereitzustellen. Einige Anbieter, die in diesem Kontext problematisch sein könnten:

Kaspersky Secure Connection: Als russisches Unternehmen unterliegt Kaspersky den lokalen Gesetzen, die eine Zusammenarbeit mit staatlichen Stellen vorschreiben.

Amnezia VPN: Obwohl Amnezia VPN ein Open-Source-Projekt ist, das von russischen Aktivisten entwickelt wurde, besteht aufgrund des Ursprungslandes das Risiko staatlicher Einflussnahme.

Rsocks: Dieser russische Proxy-Dienst wurde 2022 vom US-Justizministerium geschlossen, nachdem bekannt wurde, dass er kompromittierte Geräte für den Verkauf von IP-Adressen nutzte.

China

China hat strikte Vorschriften für VPN-Dienste, die eine umfassende Überwachung und Zensur ermöglichen. Einige bekannte Anbieter mit Verbindungen zu China:

Turbo VPN und VPN Proxy Master: Diese Dienste sind mit dem chinesischen Unternehmen Qihoo 360 verbunden, das von den USA aufgrund militärischer Verbindungen sanktioniert wurde.

X-VPN und Tachyon VPN: Diese Dienste wurden von russischen Behörden blockiert, was auf mögliche Sicherheitsbedenken hindeutet.

USA

Obwohl die USA als demokratischer Rechtsstaat gelten, ermöglichen Gesetze wie der Patriot Act staatlichen Stellen den Zugriff auf Nutzerdaten. Einige US-amerikanische VPN-Anbieter, bei denen Vorsicht geboten ist:

Hotspot Shield (AnchorFree): Das Unternehmen hat Niederlassungen in den USA, der Ukraine und Russland. Es gab in der Vergangenheit Bedenken hinsichtlich der Privatsphäre und der Zusammenarbeit mit Behörden.

HMA (HideMyAss!): Obwohl HMA eine No-Logs-Politik eingeführt hat, wurde das Unternehmen 2019 von russischen Behörden aufgefordert, sich einem staatlichen Zensurregister anzuschließen.

Private Internet Access (PIA): PIA wurde 2019 von Kape Technologies übernommen, einem Unternehmen mit umstrittener Vergangenheit. Obwohl PIA eine No-Logs-Politik verfolgt, gab es Bedenken hinsichtlich der Transparenz und des Datenschutzes.

Fazit - Die Wahl des richtigen VPN-Anbieters ist entscheidend für Ihre Online-Sicherheit. Vermeiden Sie Dienste aus Ländern mit restriktiven Internetgesetzen oder fragwürdigen Datenschutzpraktiken, um Ihre Daten vor unbefugtem Zugriff zu schützen. Setzen Sie stattdessen auf vertrauenswürdige Anbieter mit transparenten Datenschutzrichtlinien.

Empfehlenswerte Quellen

Wikipedia: Virtuelles Privates Netzwerk (VPN)
https://de.wikipedia.org/wiki/Virtual_Private_Network

Bundesamt für Sicherheit in der Informationstechnik (BSI): VPN-Nutzung
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Router-WLAN-VPN/Virtual-Private-Networks-VPN/virtual-private-networks-vpn.html

Golem.de: Virtual Private Network
https://www.golem.de/specials/vpn/

Die Wahrheit über VPNs
https://www.youtube.com/watch?v=IDpfCWEjbV4

Tor – Die Zwiebel unter den Netzwerken

Schützt dich... und manchmal auch die Falschen

Stell dir das Internet wie ein riesiges Straßennetz vor. Auf der Überholspur rasen Datenpakete im Ferrari von Amazon zu Google. VPN-Nutzer cruisen im dunklen Lieferwagen mit getönten Scheiben über die Nebenstraßen. Und ganz hinten, versteckt unter einem Tarnnetz, tuckert ein alter Bus, der alle paar Kilometer die Route ändert – willkommen im Tor-Netzwerk.

Was ist Tor überhaupt – und warum so geheimnisvoll?

Tor steht für „The Onion Router“, benannt nach seiner schichtweisen Verschlüsselung – wie bei einer Zwiebel. Entwickelt wurde es ursprünglich vom US-Militär, um die Kommunikation von Diplomaten und Journalisten abhörsicher zu machen. Heute ist es ein Open-Source-Projekt, das vor allem eines will: Anonymität im Netz.

Und das funktioniert so: Deine Internetanfrage wird in mehrere Schichten Verschlüsselung gepackt (Zwiebel-Style) und über drei zufällige Server (sogenannte „Nodes“) geschickt. Jeder kennt nur seinen Vorgänger und seinen Nachfolger – das bedeutet: Niemand weiß, wer du bist oder was du machst. Klingt nach James Bond, ist aber Open Source.

Warum ist Tor so langsam?

Stell dir vor, du willst von München nach Hamburg – aber dein Weg führt dich erst über Paris, dann Warschau, und dann erst an dein Ziel. Kein Wunder, dass dein Datenpaket dabei ins Schnaufen kommt. Die langen Umwege, die mehrfache Verschlüsselung und die freiwillig betriebenen Server (oft ohne Supercomputer-Power) sorgen für Geschwindigkeit auf Schnecken-Niveau. Privatsphäre hat eben ihren Preis – und manchmal dauert sie.

Das Darknet – wo die Zwiebel richtig düster wird

Jetzt wird's ernst – denn das Tor-Netzwerk ermöglicht nicht nur anonymes Surfen, sondern auch den Zugang zum sogenannten Darknet. Dort finden sich Websites mit der Endung .onion, die nur über den Tor-Browser erreichbar sind.

Und hier ist die Zwiebel bitter:

Tor schützt nicht nur Whistleblower, Journalisten und Dissidenten – sondern auch Kriminelle.

Im Darknet tummeln sich:

- Schwarzmärkte für Drogen, Waffen oder gestohlene Daten
- Hackerforen
- Foren für Cybercrime-Dienstleistungen („Hacken auf Bestellung")
- Illegale Pornografie

Und vieles mehr, dass man lieber nicht im Browserverlauf hat!

Tor selbst ist nicht illegal – das Netzwerk ist ein Werkzeug.

Doch wie bei einem Küchenmesser kommt es darauf an, wofür man es benutzt. Der Schutz der Privatsphäre ist legitim und wichtig, aber die Technologie wird eben auch von Leuten genutzt, die lieber nicht erkannt werden wollen – aus den falschen Gründen.

Kann man beim Tor-Netzwerk den Ausgangspunkt bestimmen?

Nicht direkt. Der Tor-Client wählt die sogenannte „Circuit" automatisch. Du kannst zwar geografische Regionen einschränken (z. B. „keine Exit-Node in den USA"), aber die Kontrolle ist begrenzt. Der Exit Node – also der letzte Knoten vor dem offenen Internet – kann den

unverschlüsselten Datenverkehr sehen. Deshalb: immer HTTPS nutzen, sonst kann jemand mitlesen, was du tippst.

Fazit - Tor ist mächtig – aber nicht ohne Risiken

Tor ist ein großartiges Werkzeug für:

- Menschen in autoritären Ländern, die staatlicher Zensur entgehen wollen
- Journalisten, die anonym mit Whistleblowern kommunizieren müssen
- Alle, die ein hohes Maß an Privatsphäre im Netz wünschen

Aber: Tor ist kein Spielzeug, und wer sich ins Darknet begibt, sollte wissen, worauf er sich einlässt. Der Grat zwischen Privatsphäre und Illegalität ist schmal – und in der falschen Nachbarschaft kann man sich auch anonym die Finger verbrennen.

Wenn du einfach nur deine Daten schützen willst, ohne tief in die digitale Unterwelt abzutauchen, ist ein vertrauenswürdiger VPN-Anbieter oft die bessere (und schnellere) Wahl. Wer aber bereit ist, die langsame Reise durch die Daten-Zwiebel anzutreten, findet im Tor-Netzwerk einen mächtigen – und manchmal auch gefährlichen – Begleiter.

Empfehlenswerte Quellen

Wikipedia: Tor (Netzwerk)
https://de.wikipedia.org/wiki/Tor_(Netzwerk)

The Tor Project – Offizielle Webseite
https://www.torproject.org/

Electronic Frontier Foundation (EFF): Einführung in Tor
https://www.eff.org/pages/tor-and-https

YouTube: Das TOR-Netzwerk ist jetzt also ÜBERWACHT?
https://www.youtube.com/watch?v=YOJabNSX4V4

YouTube: How TOR works
https://www.youtube.com/watch?v=79m7mX3rC8Q

Sichere Passwörter

Warum sie wichtig sind und wie du sie dir merken kannst

In einer Welt, in der Cyberangriffe, Datenlecks und Identitätsdiebstahl fast alltäglich geworden sind, sind starke Passwörter wichtiger denn je. Ein gutes Passwort ist wie ein solider Türschlüssel – nur dass es nicht dein Haus schützt, sondern dein digitales Leben.

Warum einfache Passwörter gefährlich sind
Viele Menschen verwenden immer noch Passwörter wie:

- 123456
- Passwort
- Qwertz
- hallo123
- oder einfach ihren Vornamen + Geburtsjahr

Solche Passwörter sind für sogenannte Brute-Force-Angriffe oder Wörterbuch-Angriffe ein Kinderspiel. Hacker nutzen riesige Listen mit den häufigsten Passwörtern – und brauchen manchmal nur Sekunden, um ein schwaches Passwort zu knacken.

Was ein gutes Passwort ausmacht
Ein starkes Passwort sollte folgende Eigenschaften haben:

- Mindestens 12–16 Zeichen lang
- Eine Kombination aus Groß- und Kleinbuchstaben
- Zahlen und Sonderzeichen
- Keine persönlichen Daten (Name, Geburtsdatum, Haustier, etc.)

- Keine echten Wörter aus dem Wörterbuch in einfacher Form

Hilfreiche Strategien für sichere Passwörter

1. Gegensätzliche Wortkombinationen

Zwei oder drei zufällige, widersprüchliche Begriffe bleiben im Gedächtnis und sind schwer zu erraten – besonders, wenn du sie noch mit Zahlen und Sonderzeichen kombinierst.

Beispiele:

- KaffeeEisPizza!1978
- WolkenHammerMario#22
- ZebraLaptop_61+Cat
- BürostuhlPizza@88PC
- BananenOga-Schwert303
- WinterPaprika!01-Fisch
- Drachen&VW+Müsli&2012

Diese Kombinationen ergeben keinen Sinn – und das ist gut so. Je absurder, desto besser. Je mehr Wörter – Sonderzeichen und Zahlen, desto besser (PizzaDemo&Pommes2025@DeadLine!c00l).

2. Zeilen aus Liedern oder Gedichten

Nimm eine Zeile, die du gut kennst, und verwandle sie in ein Passwort, indem du die Anfangsbuchstaben jedes Wortes nimmst und einige Zahlen/Sonderzeichen einbaust.

Beispiel aus einem Lied:

„Die Gedanken sind frei, wer kann sie erraten?“
→ Dgsf!Wkse?1820

Oder aus einem Gedicht:

„Ein Männlein steht im Walde ganz still und stumm“
→ EMsiWgsus!24

Das Ergebnis ist kryptisch für andere – aber für dich gut merkbar.

3. Eigene Merksätze

Denke dir einen Satz aus, den nur du verstehst, und nutze jeweils die Anfangsbuchstaben oder Abkürzungen.

Beispiel:

„Meine Katze schläft immer auf dem Router, wenn ich arbeite.“
→ MksiadRwia!

Oder
„Ich esse donnerstags 3 Kekse mit Senf und Vanille-Eis.“
→ Ied3KmSuVE!

Auch hier gilt: Was für andere keinen Sinn ergibt, kann für dich leicht einprägsam sein.

Was du vermeiden solltest

- Namen (eigene oder von Familie, Haustieren, Promis)
- Geburtsdaten oder Telefonnummern
- Wiederholungen: aaaa1111
- Tastaturmuster: qwertz, asdfgh
- Ein einziges Passwort für alles verwenden

Wenn ein Dienst gehackt wird und du dasselbe Passwort überall nutzt, sind auch deine anderen Konten kompromittiert.

Deshalb: für jeden Dienst ein eigenes Passwort.

Passwortmanager – dein digitales Notizbuch

Wenn du denkst: „Wie soll ich mir so viele Passwörter merken?“, ist ein Passwortmanager die Lösung. Damit speicherst du alle Passwörter sicher an einem Ort – verschlüsselt.

Du brauchst nur ein einziges starkes Master-Passwort, zum Beispiel:

- KeksMond#2025!DL
- 99Lampen!Tiger&PingPong

Nutze niemals dasselbe Passwort für deinen Passwortmanager wie für andere Dienste!

Fazit - Einfachheit ist bequem – aber gefährlich! Ein gutes Passwort ist nicht bequem – aber sicher. Es schützt nicht nur dein E-Mail-Konto, sondern auch deine Online-Bank, deine Cloud-Fotos und deine Identität. Investiere ein paar Minuten Zeit, um deine Passwörter zu überarbeiten. Das ist deutlich einfacher als der Ärger nach einem Hack.

Empfehlenswerte Quellen

Wikipedia: Passwort
https://de.wikipedia.org/wiki/

Bundesamt für Sicherheit in der Informationstechnik (BSI): Empfehlungen für sichere Passwörter
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

Have I Been Pwned?: Datenbank für geleakte Passwörter
https://haveibeenpwned.com/Passwords

Passwörter verwalten mit einem Passwort-Manager
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Passwort-Manager/passwort-manager_node.html

YouTube: Unknackbar aber einfach zu merken! - Passwörter Einfach Erklärt (1/5)
https://www.youtube.com/watch?v=jtFc6B5lmIM

YouTube: Sichere Passwörter | BSI
https://www.youtube.com/watch?v=cqE1djdxipc

Passwort-Manager im Vergleich

Wie du deine digitalen Schlüssel sicher und bequem verwalten kannst

In der heutigen digitalen Welt brauchst du für nahezu alles ein Passwort: Online-Banking, soziale Netzwerke, Streaming-Dienste, Shopping-Portale – und vielleicht sogar noch für die digitale Kaffeemaschine. Je mehr Dienste wir nutzen, desto größer wird der Passwort-Dschungel. Und wer ehrlich ist, weiß: Die meisten Menschen nutzen entweder ein zu einfaches Passwort – oder immer dasselbe.

Das Problem:

Ein gutes Passwort sollte einzigartig, komplex, lang – und vor allem: nicht leicht zu erraten sein.

Aber wer soll sich all diese kryptischen Zeichenketten merken?

Die Antwort: Ein Passwort-Manager.

Er speichert deine Passwörter sicher, verschlüsselt und auf Wunsch auch geräteübergreifend – damit du dich nur noch ein einziges Master-Passwort merken musst.

Doch welche Passwort-Manager sind wirklich sicher, seriös und für dein System geeignet?

Bevor wir uns konkrete Anbieter anschauen, ein kurzer Blick auf die wichtigsten Merkmale:

- **Ende-zu-Ende-Verschlüsselung:** Deine Daten werden lokal verschlüsselt und erst beim Entsperren entschlüsselt. Selbst der Anbieter kann nichts einsehen.
- **Zero-Knowledge-Architektur:** Der Anbieter weiß weder deine Passwörter noch dein Master-Passwort.
- **Zwei-Faktor-Authentifizierung (2FA):** Für zusätzliche Sicherheit beim Login.
- **Automatisches Ausfüllen:** Passwörter, Kreditkarten oder Formulare mit einem Klick ausfüllen.
- **Plattformübergreifend:** Synchronisation zwischen Smartphone, Tablet, PC etc.
- **Backup-Möglichkeiten & Notfallzugriff:** Für den Fall, dass du dein Master-Passwort verlierst.

Die besten vertrauenswürdigen Passwort-Manager im Vergleich

1. Bitwarden – Die Open-Source-Legende

Sicherheit: Open Source, Zero-Knowledge, regelmäßige Audits

Funktionen: Passwort-Tresor, 2FA, Passwortgenerator, Organisationen/Familien

Kosten: Kostenlos mit optionaler Premium-Version (ca. 10 €/Jahr)

Betriebssysteme:

- Windows
- macOS
- Linux
- Android

- iOS

Browser: Chrome, Firefox, Safari, Edge, Opera, Brave

Für wen geeignet?

Für alle, die auf Transparenz, Datenschutz und Plattformvielfalt setzen. Bitwarden ist besonders bei sicherheitsbewussten Nutzern, IT-Fachleuten und Open-Source-Fans beliebt.

2. 1Password – Komfort trifft Sicherheit

Sicherheit: Verschlüsselung auf hohem Niveau, kein Zugriff auf deine Daten durch den Anbieter

Funktionen: Watchtower (Sicherheitscheck), 2FA, sichere Notizen, Reise-Modus

Kosten: Nur als Abo-Modell, ca. 3 €/Monat (Einzelnutzer), Familien-/Business-Tarife verfügbar

Betriebssysteme:

- Windows
- macOS
- Linux
- Android
- iOS

Browser: Chrome, Firefox, Safari, Edge

Für wen geeignet?

Für Nutzer, die ein elegantes Design und starke Features wollen – besonders geeignet für Familien oder Teams, die Passwörter gemeinsam verwalten möchten.

3. Dashlane – Der Komfort-Profi

Sicherheit: AES-256-Verschlüsselung, Zero-Knowledge-Architektur

Funktionen: Automatischer Passwortwechsel, Dark-Web-Überwachung, 2FA, VPN (Premium)

Kosten: Kostenlos (eingeschränkt), Premium-Version ab ca. 4 €/Monat

Betriebssysteme:

- Web-App (alle Browser)
- Android
- iOS

Desktop-Apps (ältere Versionen noch verfügbar, Fokus jetzt auf Web-App)

Für wen geeignet?

Für alle, die sich nicht mit Technik aufhalten wollen, sondern eine praktische All-in-One-Lösung suchen – inklusive Passwortverwaltung, Sicherheitswarnungen und VPN.

4. KeePass – Der Offline-Klassiker

Sicherheit: Offline, Open Source, extrem flexibel, viele Plugins verfügbar

Funktionen: Manuelle Verwaltung, Verschlüsselung durch Master-Passwort oder Schlüsseldateien

Kosten: Komplett kostenlos

Betriebssysteme:

- Windows (Original)
- macOS (über KeePassXC)
- Linux (KeePassXC, KeePassX)
- Android (KeePass2Android, KeepassDX)
- iOS (Strongbox, KeePassium)

Für wen geeignet?

Für Technikliebhaber und Puristen, die ihre Daten lieber lokal speichern. Ideal, wenn du Cloud-Diensten nicht traust oder absolute Kontrolle willst.

5. Proton Pass – Der Datenschutz-Neuling

Sicherheit: Schweiz-basierter Anbieter, Zero-Knowledge, Ende-zu-Ende-Verschlüsselung, Open Source

Funktionen: Passwortmanager, E-Mail-Aliase, integrierbar mit ProtonMail/VPN

Kosten: Kostenloser Plan, Premium ab ca. 4 €/Monat

Betriebssysteme:

- Android
- iOS
- Browser: Chrome, Firefox, Brave, Edge

Desktop (Beta/Entwicklung geplant)

Für wen geeignet?

Für alle, denen Datenschutz besonders wichtig ist – und die Proton bereits für Mail oder VPN nutzen. Noch in der Weiterentwicklung, aber vielversprechend.

Fazit - Welcher Passwort-Manager ist der richtige für dich?

Das hängt von deinem Techniklevel, deinem Budget und Sicherheitsbedürfnissen ab:

- Maximale Kontrolle, keine Cloud: KeePass
- Viel Leistung, Open Source: Bitwarden
- Stark für Familien & Teams: 1Password
- Komfort-Lösung mit Extras: Dashlane
- Datenschutz aus der Schweiz: Proton Pass

Empfehlenswerte Quellen

Wikipedia: Passwort-Manager
https://de.wikipedia.org/wiki/Passwort-Manager

Bitwarden – Offizielle Webseite
https://bitwarden.com/

1Password – Offizielle Webseite
https://1password.com/

Dashlane – Offizielle Webseite
https://www.dashlane.com/

KeePass – Offizielle Webseite
https://keepass.info

Proton Pass – Proton AG
https://proton.me/pass

YouTube: Cyber-Sicherheit² - Wie verwalte ich sichere Passwörter? | BSI
https://www.youtube.com/watch?v=X9blxJ4Sa2A

Das Smartphone hört mit

Manchmal mehr, als dir lieb ist

„Wir haben doch nur über Schuhe geredet!“
„Ich hab’s nicht mal gegoogelt!“
„Wieso zeigt mir Instagram jetzt genau DIE Sneaker an?!“

Wenn dir das bekannt vorkommt, bist du nicht allein. Immer mehr Menschen berichten von einem seltsamen Phänomen: Man spricht ganz beiläufig über ein bestimmtes Produkt – sagen wir, neue Laufschuhe – und kurz darauf erscheint genau dieses Modell als Werbeanzeige in der Lieblings-App.

Zufall? Einbildung? Oder hört das Smartphone tatsächlich mit?
Das Mikrofon: Immer da, immer wachsam?

Moderne Smartphones sind mit einer leistungsstarken Spracherkennung ausgestattet. Sprachassistenten wie Siri, Google Assistant oder Alexa (bei entsprechender App) sind so programmiert, dass sie ständig „lauschen“, um auf ihre Aktivierungswörter wie „Hey Siri“ oder „Okay Google“ zu reagieren.

Diese Technologie nennt sich Hotword Detection. Dabei wird das Mikrofon in einen energieeffizienten „Wachzustand“ versetzt, der nur kleine Sprachmuster analysiert. Sobald das Aktivierungswort erkannt wird, springt die komplette Spracherkennung an und beginnt, dein gesprochenes Wort aufzunehmen und zu analysieren.

Was viele nicht wissen: Damit das funktioniert, muss das Mikrofon ständig zuhören – wenn auch angeblich lokal auf dem Gerät und ohne

Datenübertragung. Aber: Wo ist die Grenze zwischen „lauschen auf Kommando“ und „beobachten, was du sagst“?

Sprachdaten für Werbung? Offiziell: Nein. Inoffiziell…?

Die großen Tech-Konzerne (Google, Apple, Meta & Co.) betonen regelmäßig, dass keine Sprachaufnahmen ohne ausdrückliche Zustimmung für Werbezwecke verwendet werden. In den AGBs steht sinngemäß: “Wir analysieren Sprache nur zur Verbesserung des Nutzererlebnisses.”

Doch das Vertrauen ist oft angekratzt – gerade, wenn man nach einem harmlosen Gespräch über „vegane Zahnpasta“ plötzlich Werbeanzeigen für „nachhaltige Bambus-Zahnbürsten“ sieht. Der Gedanke liegt nahe: Hat mein Smartphone etwa mitgehört?

Kurioser (aber realer) Alltag:

Du erzählst deiner Freundin, dass du dringend neue Sportschuhe brauchst. Du erwähnst sogar die Marke. Eine halbe Stunde später öffnest du Facebook – Boom, die exakt gleichen Schuhe grinsen dich in der Anzeige an.

Du hast nichts gegoogelt. Nichts gesucht. Nur gesprochen.
Zufall? Vielleicht.

Cleveres Data-Tracking über deine Apps, dein Standort, deine App-Nutzung und deine Kontakte? Sehr wahrscheinlich.

Oder: Hat da wirklich das Mikrofon zugehört?

Noch schlauer: Mikrovibration statt Mikrofon

Was wie aus einem Spionagefilm klingt, ist technisch längst möglich – und sogar wissenschaftlich belegt:

Smartphones können Sprache erkennen, ohne das Mikrofon zu benutzen.

Wie das geht?

Moderne Smartphones sind vollgepackt mit Sensoren – darunter auch Beschleunigungssensoren (Accelerometer) und Gyroskope. Diese Sensoren sind ursprünglich dafür gedacht, Bewegungen zu erkennen (z. B. beim Drehen des Bildschirms oder beim Schrittzählen).

Forscher haben jedoch herausgefunden, dass diese Sensoren auch Mikrovibrationen aufzeichnen können, die durch Schallwellen – also Sprache – entstehen. Selbst wenn du das Handy auf einem Tisch neben dir liegen hast und ganz normal sprichst, vibriert die Tischplatte ganz leicht. Und diese winzigen Bewegungen reichen aus, um mit Hilfe von KI erstaunlich gut zu rekonstruieren, was gesagt wurde – sogar ohne Mikrofonaktivität.

Ein berühmtes Beispiel:

In einem Experiment konnten Forscher aus Stanford mithilfe der eingebauten Sensoren und intelligenter Software Worte mit bis zu 80 % Genauigkeit erkennen, ohne dass das Mikrofon verwendet wurde.

Der Trick: Die Software analysierte, wie der Tisch (auf dem das Handy lag) auf bestimmte Sprachfrequenzen reagierte.

Kurz gesagt: Selbst wenn du das Mikrofon deaktivierst – Sensoren könnten trotzdem mithören, zumindest theoretisch.

Datenschutz: Was passiert mit deinen Daten?

Ob bewusst oder unbewusst, unsere Smartphones sammeln rund um die Uhr Daten:

- Standort
- App-Nutzung
- Bewegungsmuster
- Touch-Eingaben
- Verweildauer bei Inhalten
- Und natürlich: Spracheingaben

Viele Apps fordern beim ersten Start Zugriff auf das Mikrofon – auch, wenn sie eigentlich gar nichts mit Sprache zu tun haben. Ein Taschenlampen-App mit Mikrofonzugriff? Sollte verdächtig wirken.

Und was passiert mit den gesammelten Daten?

Oft landen sie bei Werbenetzwerken, die daraus ein ziemlich genaues Profil von dir erstellen können. Sie wissen, dass du letzte Woche zweimal nach einem Laufband gesucht hast, dass du gerne Katzenvideos magst, und dass du letzte Nacht um 2:00 Uhr bei Google „bester Döner in der Nähe“ eingegeben hast.

Was kann ich dagegen tun?

1. Mikrofonrechte überprüfen:
Gehe regelmäßig in die Einstellungen deines Smartphones und schau nach, welche Apps Zugriff auf das Mikrofon haben. Entziehe unnötigen Apps diesen Zugriff.

2. Sprachassistenten deaktivieren:

Wenn du Siri oder Google Assistant nicht nutzt, kannst du die Spracherkennung komplett abschalten.

3. App-Berechtigungen hinterfragen:

Warum braucht eine Spiele-App Zugriff auf deinen Standort und dein Mikrofon? Sei kritisch.

4. Sensorzugriffe einschränken:

Einige Android-Versionen ermöglichen inzwischen auch die Kontrolle über Bewegungssensoren. Auch hier lohnt sich ein Blick.

5. Werbetracking begrenzen:

In den Systemeinstellungen vieler Geräte kannst du personalisierte Werbung deaktivieren. Das verhindert nicht die Datensammlung – aber reduziert gezielte Werbung.

Fazit - Dein Smartphone hört mehr zu, als es sagt! Ob über Mikrofon oder Sensoren – dein Smartphone ist kein passiver Begleiter, sondern ein aktives, lernendes Gerät. Es sammelt Daten, wertet Verhalten aus – und ja, unter bestimmten Umständen kann es auch „mitlauschen". Und selbst wenn das nicht direkt über Sprache geschieht, kombinieren smarte Systeme heute viele verschiedene Quellen: Standort, Browsing-Verhalten, soziale Netzwerke, Sensoren.

Dass Werbung oft so treffsicher ist, liegt nicht unbedingt an Spionage – sondern an sehr effizientem Datenabgleich und cleverem Marketing.

Trotzdem: Ein bewusster und kritischer Umgang mit Berechtigungen, Einstellungen und digitalen Assistenten ist mehr als angebracht. Denn auch wenn dein Smartphone kein richtiger Lauscher

ist – es merkt sich vieles, das du vielleicht lieber für dich behalten würdest.

Empfehlenswerte Quellen

A deep-dive into Hot Word Detection and Zero-Few Shot Learning
https://antematter.io/blogs/hot-word-detection-and-zero-shot-learning

BBC: Why phones that secretly listen to us are a myth
https://www.bbc.com/news/technology-49585682

Gyrophone: Recognizing Speech From Gyroscope Signals
https://www.blackhat.com/docs/eu-14/materials/eu-14-Nakibly-Gyrophone-Eavesdropping-Using-A-Gyroscope-wp.pdf

YouTube: Können iPhone und Android Handys heimlich mithören? Wir programmieren Apps, um das zu beweisen!
https://www.youtube.com/watch?v=rX2tK-qSVpk

Die unsichtbare Rechnung

Warum kostenlose Apps selten wirklich kostenlos sind

Du lädst dir eine App herunter – sie ist kostenlos, hat viele gute Bewertungen und macht genau das, was du brauchst: ein bisschen Fitness, ein bisschen Spaß, vielleicht ein Foto-Editor oder ein Spiel für zwischendurch.

Aber schon nach ein paar Minuten kommt die erste Werbeeinblendung.

Und du fragst dich: Wie verdienen die Entwickler eigentlich ihr Geld?

Die Antwort lautet meist: Mit dir.

Kostenlos ist selten umsonst!

Was viele Nutzer unterschätzen:

Wenn eine App nichts kostet, wird sie höchstwahrscheinlich durch Werbung oder Datenweitergabe finanziert.

Das bedeutet:

- Du wirst mit Werbeanzeigen bombardiert,
- deine App-Nutzung wird analysiert,
- und dein Verhalten wird akribisch aufgezeichnet.

Nicht die App ist das Produkt – **DU** bist es.

Wie kostenlose Apps Geld mit dir verdienen
Werbung:

Viele Apps nutzen Werbenetzwerke wie Google AdMob oder Facebook Audience Network, um dir Werbung anzuzeigen. Jedes Mal, wenn du klickst oder die Anzeige nur siehst, verdient der Entwickler ein paar Cent.

Tracking & Datenverkauf:

Noch lukrativer ist es, wenn die App dich trackt:

- Welche Seiten du besuchst.
- Wo du dich aufhältst.
- Welche Interessen du hast.
- Was du wann und wie oft nutzt.

Diese Daten werden dann an Datenhändler oder Werbeunternehmen verkauft – oft anonymisiert, aber dennoch mit einem ziemlich genauen Nutzerprofil.

Hintertürchen in den Berechtigungen:

Viele Apps fordern Berechtigungen, die sie eigentlich gar nicht brauchen: Zugriff auf Mikrofon, Kamera, Kontakte, Standort. Und wer liest schon jede Berechtigungsabfrage wirklich durch?

Auch kostenpflichtige Apps können gefährlich sein

Ein weitverbreiteter Irrtum: „Wenn ich für eine App bezahle, dann ist sie sicher.“

Leider nicht immer.

Beispiele:

FaceApp: Diese beliebte Foto-App, die dein Gesicht altern lässt, kommt aus Russland und sammelt viele Daten – auch von Nutzern der Bezahlversion. Dazu gehören Metadaten deiner Fotos, Gerätestandort und Gesichtserkennungsmuster.

: Diese Scanner-App war jahrelang beliebt – bis Sicherheitsforscher feststellten, dass eine Version Schadcode enthielt, der Hintertüren für Werbetracker und sogar Malware öffnete.

Weather Forecast Apps: Mehrere Wetter-Apps – darunter auch einige kostenpflichtige – wurden dabei erwischt, Standortdaten im Hintergrund zu erfassen und an Datenhändler zu verkaufen, ohne dies klar offenzulegen.

TikTok: Zwar kostenlos, aber extrem datenhungrig. Die App speichert u. a. Gerätedaten, Bewegungsmuster, Tastatureingaben, und sammelt Daten auch dann, wenn du sie gerade gar nicht benutzt. Auch mit einem bezahlten TikTok-Abo bleibt das Tracking aktiv.

Problematische Beispiele aus der Praxis

XRecorder: Ein Bildschirmaufnahme-Tool, das Nutzerdaten an bis zu 15 Drittfirmen weitergibt – darunter auch chinesische Analysefirmen.

DU Battery Saver: Eine App, die angeblich deine Akkulaufzeit verlängert, wurde dabei erwischt, Daten im Hintergrund zu sammeln, sogar ohne dass der Nutzer die App aktiv benutzt hat.

Photo Vault-Apps: Viele „versteckte Galerie“-Apps, die Privatsphäre suggerieren, greifen trotzdem auf Kontakte, Standort und Gerätespeicher zu – und verschicken sogar App-Nutzungsdaten an Server in Ländern mit fragwürdigen Datenschutzstandards.

Warum Werbung in Apps ein Risiko ist

Viele denken: „Werbung nervt zwar, aber schadet ja nicht.“

Das Problem ist: Moderne Werbeplattformen sind keine simplen Anzeigen mehr.

Sie beinhalten oft:

- Tracking-Skripte
- Fingerprinting-Technologien
- Cross-App-Tracking, das dich über mehrere Apps hinweg beobachtet
- Zugriffe auf Mikrofon oder Kamera (manche Werbebibliotheken versuchen sogar, Umgebungsgeräusche auszuwerten)

Selbst wenn du keine Werbung anklickst, wird gemessen, wie lange du sie siehst, wie du scrollst, ob du wegschaltest – und daraus wird ein Profil erstellt.

Auch App-Stores sind nicht perfekt

Google Play und Apple App Store prüfen zwar Apps vor der Veröffentlichung – doch immer wieder schaffen es Apps mit verstecktem Code, Tracker-Modulen oder Malware durch die Kontrollen. Besonders gefährdet sind:

- Free-to-play-Games mit vielen In-App-Käufen
- VPN-Apps aus unbekannter Herkunft
- Taschenlampen- und Wallpaper-Apps mit überzogenen Berechtigungen

Wie du dich schützen kannst

- Nur Apps aus vertrauenswürdiger Quelle installieren
- Lies Bewertungen, Recherchiere den Anbieter, prüfe, ob die Firma existiert.
- App-Berechtigungen prüfen und einschränken
- Braucht ein Spiel wirklich Zugriff auf dein Mikrofon? Oder eine Notiz-App Zugriff auf deinen Standort?
- Apps regelmäßig aufräumen
- Lösche Apps, die du nicht mehr benutzt. Weniger Apps = weniger potenzielle Spionage.
- Werbung blockieren (wo erlaubt)
- Ein seriöser Werbeblocker oder ein VPN mit integrierter Tracker-Blockade kann helfen, viele Werbenetzwerke zu unterbinden.

- Verzichte auf Bequemlichkeit bei sensiblen Daten
- Banking-, Gesundheits- oder Kommunikations-Apps sollten immer von bekannten und vertrauenswürdigen Anbietern stammen – keine No-Name-App mit 4,9 Sternen und 300 Bewertungen aus „Zufallsländern".

Fazit - Kostenlos kann teuer werden! Der Preis für eine kostenlose App ist oft deine Privatsphäre. Ob Werbung, Tracker, Datenweitergabe oder versteckte Funktionen – viele Apps verfolgen dich unbemerkt. Und selbst kostenpflichtige Apps sind keine Garantie für Datenschutz.

Sei kritisch. Stell Fragen. Lies Berechtigungen. Und denk daran: Wenn du für eine App nicht mit Geld bezahlst, zahlst du wahrscheinlich mit deinen Daten.

Empfehlenswerte Quellen

What is monetization for mobile apps?
https://www.adjust.com/glossary/app-monetization/

Was ist Website-Tracking und wie funktioniert es?
https://www.dr-datenschutz.de/was-ist-website-tracking-und-wie-funktioniert-es/

Bundesamt für Sicherheit in der Informationstechnik (BSI): Sicherheit bei Apps
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Basisschutz-fuer-Computer-Mobilgeraete/Schutz-fuer-Mobilgeraete/Sicherheit-bei-Apps/sicherheit-bei-apps_node.html

Apps und Datenschutz - so geizen Sie mit Ihren Daten
https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/apps-und-datenschutz-so-geizen-sie-mit-ihren-daten-6431

Diese Risiken gehen Sie ein, wenn Sie kostenlose Apps nutzen
https://www.ksta.de/redaktion/risiko-bei-kostenlosen-apps-das-ist-der-wahre-preis-von-gratis-programmen-194868

Datenschutz bei Apps: Worauf man achten sollte
https://www.addpriv.eu/datenschutz-bei-apps/

Von Cent-Schnäppchen und Klickrausch

Wie Temu & Co. uns zu Billigshoppern erziehen (und warum das ein Problem ist)

Es fängt immer ganz harmlos an.

Ein Freund sagt: „Ey, guck mal, ich hab bei Temu zehn Handyhalterungen für 3,20 € bekommen. Versand kostenlos!“

Du runzelst die Stirn, klickst – und drei Tage später hast du nicht nur eine Handyhalterung bestellt, sondern auch blinkende LED-Socken, ein Katzenkostüm (obwohl du keinen Kater hast), fünf Paar Hausschuhe und eine Zitronenpresse in Elefantenform.

Willkommen in der wunderbaren Welt des Billigshoppings aus Fernost – mit kostenlosen Versandversprechen, absurden Rabatten und einer Benutzeroberfläche, die so optimiert ist, dass du gar nicht merkst, wie du in einen Kaufrausch rutschst.

Was macht Apps wie Temu und AliExpress so verlockend?

Psychologische Tricks vom Feinsten

Die Apps sind wie kleine digitale Casinos – statt blinkenden Spielautomaten gibt es „Flash Deals“, „Mega-Angebote“ und täglich neue Glücksrad-Gewinne. Du klickst nicht nur, du spielst.

Das Gehirn schüttet Dopamin aus – wie bei einem Jackpot. Und schon fühlt sich das nächste 1,39 €-Gadget an wie ein Triumph.

Preise, die zu gut sind, um wahr zu sein
Und meistens sind sie es auch.

Du bekommst ein Produkt für unter einem Euro, mit kostenlosem Versand aus China? Da weißt du insgeheim, dass irgendwo jemand dabei draufzahlt – wahrscheinlich du, in Form von Qualität, Service oder Datenschutz.

Alles wirkt dringlich
Die Uhr tickt. Das Angebot läuft gleich ab. Nur noch 3 Stück auf Lager! Sei Schnell, der Otto hat schon eins davon im Warenkorb!

Diese künstliche Verknappung sorgt dafür, dass wir schneller kaufen und weniger nachdenken. Der Impuls siegt – der Verstand wird auf später verschoben.

Warum das ein Problem ist – für dich und für alle anderen

1. Die Illusion des Sparens
Natürlich sieht es so aus, als würdest du Geld sparen. Aber wer fünfmal 3 € ausgibt für Dinge, die er gar nicht braucht, hat am Ende trotzdem 15 € weniger – und kein Produkt davon hält wahrscheinlich länger als der Versand gedauert hat.

„Günstig gekauft ist oft doppelt bezahlt“ – sagt nicht nur Oma, sondern auch dein Konto nach drei Monaten Temu-Exzessen.

2. Die lokale Wirtschaft leidet
Kleine Läden in deiner Stadt, regionale Online-Shops, lokale Startups – sie können nicht mithalten mit Preisen, bei denen das Porto allein hierzulande mehr kosten würde als das ganze Produkt bei AliExpress.

Das Problem:

- Die Wertschöpfung findet nicht mehr vor Ort statt.
- Steuern fließen ins Ausland.
- Und faire Arbeitsbedingungen? Nun ja, die sind in vielen chinesischen Produktionsstätten eher ein Vorschlag als Realität.

Während dein lokaler Schuhladen Mitarbeiter bezahlen, Miete stemmen und faire Lieferketten erhalten muss, schickt dir eine riesige Plattform ein Paar „High-Speed Sneakers“ für 5,99 €, das aussieht wie Adidas – aber riecht wie Lösungsmittel.

3. Umwelt? Ach, die auch noch…

Kleinteilig verpackte Billigprodukte werden per Luftfracht oder Containerschiff um die halbe Welt geschickt – nur damit du einen Tassenwärmer mit Glitzerlicht bekommst, der nach zwei Wochen den Geist aufgibt.

- Die CO_2-Bilanz? Miserabel.
- Verpackung? Meist Kunststoff in mehreren Schichten.
- Rückgabe? Nicht vorgesehen oder so kompliziert, dass man’s gleich lässt.

Und warum ist das Ganze so verführerisch?

- Weil es bequem ist.
- Weil die Apps gamifiziert sind.
- Weil wir gelernt haben: Mehr ist besser – und schneller ist am besten.

- Und weil du mit jedem Klick auf „Zum Warenkorb hinzufügen“ das Gefühl hast, clever zu handeln.

Dabei wirst du Schritt für Schritt konditioniert, wie der Hund von Pavlov – nur eben nicht mit Glocke, sondern mit Push-Benachrichtigung: „Du hast einen 90 %-Gutschein gewonnen!“

Ein echtes Beispiel: Der Temu-Loop

- Du bestellst einen Artikel für 1,80 €.
- Du bekommst 10 % Rabatt für deine erste Bestellung.
- Du bekommst Punkte.
- Du bekommst einen „Freunde einladen und verdienen“-Link.
- Du bekommst Benachrichtigungen, dass du bald ein Gratisgeschenk bekommst, wenn du nur noch EINE Kleinigkeit kaufst…

Herzlichen Glückwunsch, du hast gerade 8 € für Dinge ausgegeben, die du weder brauchst noch behalten wirst – und das nur, weil du dachtest, du würdest etwas gewinnen.

Fazit: Ein Klick zu viel kann teuer werden – auch wenn’s billig aussieht

Apps wie Temu und AliExpress nutzen moderne psychologische Mechanismen, um aus Nutzern dauerhafte Konsumenten zu machen – mit möglichst wenig kritischem Hinterfragen.

Das eigentliche Problem ist nicht das einzelne Schnäppchen – sondern die dauerhafte Verschiebung von Werten:

- Statt Qualität zählt Quantität.
- Statt Regionalität zählt Versandgeschwindigkeit.
- Statt Nachhaltigkeit zählt der Preis auf den ersten Blick.

Und der Preis, den wir dafür zahlen, ist nicht nur finanziell, sondern auch gesellschaftlich und ökologisch spürbar – ganz besonders für kleine, lokale Anbieter, die gegen diese Plattformen kaum eine Chance haben.

Wenn du also das nächste Mal eine Plastikbanane mit integriertem Zahnstocherhalter für 0,87 € in den Warenkorb legst, frag dich kurz:

„Brauche ich das wirklich – oder hat die App mir das eingeredet?“

Und vielleicht lohnt sich ja der Besuch im echten Laden um die Ecke – da gibt's zwar keine Gratis-Geschenke, aber ein ehrliches Gespräch, ein echtes Lächeln und Produkte, bei denen du weißt, woher sie kommen.

Bemerkenswerte Quellen

Wikipedia: Temu (E-Commerce-Plattform)
https://en.wikipedia.org/wiki/Temu

Wikipedia: AliExpress
https://de.wikipedia.org/wiki/AliExpress

Handelsblatt: Warum Temu und Shein den Onlinehandel revolutionieren – und gefährden
https://www.handelsblatt.com/unternehmen/handel-konsumgueter/china-das-machen-temu-und-shein-richtig/100063922.html

So funktioniert die neue Billig-Plattform "Temu" aus China
https://www1.wdr.de/nachrichten/temu-china-shopping-100.html

Was steckt hinter Temu? – Ein Blick hinter die Kulissen des Billig-Giganten
https://gruendertalk.com/was-steckt-hinter-temu/

Warum Billigprodukte und Eigenmarken immer teurer werden
https://www1.wdr.de/nachrichten/cheapflation-warum-billigprodukte-teurer-werden-100.html

Browser – Das Tor zum Internet

(und manchmal auch zur eigenen Privatsphäre)

Wenn das Internet ein gigantisches Einkaufszentrum voller Informationen, Videos, Nachrichten, Katzenbilder und Online-Shops ist – dann ist der Browser das Fahrzeug, mit dem du dich durch dieses digitale Shoppingcenter bewegst. Egal ob du Chrome, Firefox, Safari, Edge oder Brave benutzt: Dein Browser ist das Fenster zur Welt.

Aber – Achtung – er ist auch ein Fenster in deine Welt. Und dieses Fenster lässt sich von außen ziemlich gut durchschauen, wenn du dich nicht schützt.

Wie alles begann: Die Geburt des Browsers

Die Geschichte der Browser beginnt 1990, als der britische Informatiker Tim Berners-Lee den allerersten Webbrowser mit dem charmanten Namen „WorldWideWeb“ (später in „Nexus“ umbenannt) entwickelte. Sein Ziel: Wissenschaftlern einen einfachen Zugang zu Dokumenten im Internet ermöglichen.

Was damals aussah wie ein einfacher Texteditor mit Links, wurde später zu einem der wichtigsten Werkzeuge der modernen Welt.

Dann kam Mosaic (1993), dann Netscape Navigator (1994), und schließlich im Jahr 1995 ein kleiner Browser namens Internet Explorer, der mit Windows ausgeliefert wurde – und dem das Internet damit so richtig den Turbo zündete.

Seitdem haben wir eine ganze Armee von Browsern bekommen:

Chrome, Firefox, Safari, Opera, Brave, Edge – sie alle konkurrieren um deine Klicks.

Was Browser eigentlich tun

Ein Browser nimmt die Informationen, die du von Webseiten abrufst – also HTML, CSS, JavaScript und Bilder – und verwandelt sie in etwas Lesbares, Klickbares, Interaktives.

Du tippst: www.katzenvideos.com

Der Browser fragt den Server nach der Seite, lädt alle Inhalte herunter – und präsentiert sie dir hübsch und geordnet. So weit, so gut. Aber hier fängt es auch schon an, interessant zu werden.

Warum man so leicht erkennen kann, wo du herkommst

Fast jede Webseite kann genau sehen:

- Von welcher Webseite du gekommen bist (das nennt sich „Referrer“).
- Welche Suchbegriffe du benutzt hast, wenn du über Google kamst.
- Welche Sprache du eingestellt hast.
- Und: Welche Seiten du vorher besucht hast, wenn du Links gefolgt bist.

Das liegt daran, dass dein Browser beim Aufruf einer neuen Seite viele Informationen automatisch mitsendet – unter anderem eben die Seite, von der du kamst. Webseitenbetreiber nutzen das, um Statistiken zu erstellen – aber auch, um Werbung gezielter auszuspielen. Stichwort: Retargeting.

Wie Webseiten deinen Computer erkennen

Hier wird's noch spannender. Beim Surfen übermittelt dein Browser automatisch:

- Den Namen deines Betriebssystems (Windows, macOS, Android, iOS...).
- Die Bildschirmauflösung.
- Die verwendete Browser-Version.
- Installierte Plugins oder Schriftarten.
- Hardwareinfos wie CPU oder GPU-Typ.

Diese Daten wirken für sich genommen harmlos. Aber in Kombination können sie einen sogenannten digitalen Fingerabdruck ergeben – also ein ziemlich einzigartiges Profil, mit dem man dich auch ohne Cookies wiedererkennen kann.

Beispiel: Du nutzt ein MacBook Air mit Firefox, Deutsch als Sprache, 1920x1080 Bildschirm, installierte Schriftarten A, B, C und hast keine Werbeblocker? Schon bist du unter Hunderttausenden Nutzern identifizierbar – und wirst beim nächsten Besuch wiedererkannt.

Werbung – und warum sie nicht nur nervt, sondern auch gefährlich sein kann

Viele Webseiten finanzieren sich durch Werbung. Das ist verständlich – Inhalte wollen bezahlt werden.

ABER: Moderne Online-Werbung ist nicht nur Werbung – sie ist ein ausgeklügeltes Tracking-System.

Die meisten Werbeanzeigen werden nicht direkt von der Webseite geladen, sondern von Drittanbietern (z. B. Google, Facebook, Amazon). Diese Werbenetzwerke setzen Cookies, lesen deine

Browserinformationen aus und verfolgen dich über mehrere Seiten hinweg.

Was bedeutet das?

- Du suchst nach Wanderschuhen auf einer Seite – und bekommst sie danach überall angezeigt.
- Du liest über Migräne – und plötzlich wird dir Schmerzmittelwerbung ausgespielt.
- Du klickst auf ein süßes Shirt – und fünf Minuten später weiß Instagram davon.

Man nennt das verhaltensbasierte Werbung. Und die weiß oft mehr über dich als dein bester Freund.

Gefährlich wird es, wenn...

- über Werbenetzwerke auch Malware oder Fake-Shops verbreitet werden.
- du unbemerkt auf Phishingseiten landest.
- dein gesamtes Onlineverhalten über Monate hinweg mitprotokolliert wird.

Wie du dich schützen kannst

Zum Glück gibt es einfache Mittel, um wieder ein bisschen mehr Kontrolle zu gewinnen:

- Nutze einen werbefreien oder datenschutzfreundlichen Browser.

- z. B. Firefox, Brave oder Safari (in Kombination mit Datenschutz-Einstellungen).
- Installiere einen Werbeblocker (uBlock Origin, Privacy Badger oder AdGuard blockieren nicht nur Werbung, sondern auch Tracker).
- Nutze den Inkognito-/Privatmodus – zumindest bei heiklen Themen.
- Deaktiviere Drittanbieter-Cookies in deinen Browsereinstellungen.
- Verwende ein VPN oder das Tor-Netzwerk, wenn du anonym bleiben möchtest.
- Halte deinen Browser aktuell – viele Angriffe erfolgen über veraltete Sicherheitslücken.

Fazit: Der Browser ist dein Freund – aber auch ein Spion, wenn du ihn lässt!

Die Browser haben das Internet groß gemacht. Ohne sie gäbe es keine Katzenvideos, keine Memes, keine nächtlichen Bestellungen von Keksformen in Flamingo-Form.

Aber sie haben auch eine Schattenseite. Sie wissen viel über dich – und übermitteln dieses Wissen bereitwillig weiter, wenn du nicht aufpasst.

Mit ein paar Klicks in den Einstellungen kannst du dich aber einigermaßen gut schützen. Denn das Internet ist wie eine große Stadt: Du kannst viel erleben – aber solltest deine Haustür nicht offen lassen und dein Portemonnaie nicht in der Gesäßtasche tragen.

Empfehlenswerte Quellen

Wikipedia: Webbrowser
https://de.wikipedia.org/wiki/Webbrowser

Wikipedia: Mosaic (Browser)
https://en.wikipedia.org/wiki/Mosaic_(web_browser)

Wikipedia: Internet Explorer
https://de.wikipedia.org/wiki/Internet_Explorer

Electronic Frontier Foundation (EFF): Surveillance Self-Defense – Browser Security
https://www.eff.org/pages/surveillance-self-defense

Mozilla Developer Network (MDN): HTTP Referrer und Fingerprinting
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referer

Wikipedia: Fingerprinting (Trackingtechnik)
https://de.wikipedia.org/wiki/Fingerprinting_(Trackingtechnik)

Tracking-Cookies: So funktionieren sie und das hilft dagegen
https://www.dirks-computerecke.de/it-sicherheit-datenschutz/tracking-cookies-blockieren.htm

Webbrowser auf Smartphones

Smartphones sind für viele Nutzer das Tor zum Internet. Über Webbrowser surft man täglich im Netz, liest Nachrichten, nutzt soziale Medien oder recherchiert. Dabei ist der Schutz der Privatsphäre entscheidend – jeder Besuch einer Website kann und wird Daten hinterlassen. Tracking bedeutet, dass das Verhalten der Nutzer beobachtet und ausgewertet wird . Werbebanner, Analyse-Skripte und Cookies erfassen etwa, welche Seiten man besucht oder welche Produkte man mag . Moderne Browser sammeln zudem oft Geräte- und Nutzerdaten (sogenanntes „Fingerprinting“), um Nutzer auch ohne Cookies wiederzuerkennen . Diese Daten werden meist für personalisierte Werbung oder Nutzeranalysen verwendet, was nicht immer im Interesse der Nutzer ist.

Wie funktioniert Web-Tracking?

Cookies und Web-Banner: Websites speichern kleine Dateien (Cookies) im Browser, die z. B. Nutzer-IDs enthalten. So kann ein Werbenetzwerk einen Besucher auf verschiedenen Seiten wiedererkennen und gezielt Werbung anzeigen .

Drittanbieter-Tracker: Viele Seiten laden externe Skripte (wie Analytik- oder Werbenetzwerke). Diese Trackingserver bauen ein Profil über besuchte Seiten auf. Selbst wenn Cookies gelöscht werden, kann moderne Browser-Fingerprinting-Technik über System- und Browser-Daten Rückschlüsse auf den Nutzer ziehen .

Tracking macht sich oft unbemerkt bemerkbar (z. B. angezeigte Werbung basierend auf früheren Besuchen). Für Einsteiger ist wichtig zu wissen: Je mehr unerwünschte Werbung und Tracker ein Browser

blockiert, desto besser wird die Privatsphäre geschützt und oft auch die Ladezeit verkürzt.

Erweiterungen für Datenschutz: Adblocker und Co.

Browser, die Erweiterungen (Plugins/Add-ons) unterstützen, erlauben es, spezielle Tools zu installieren.

Typischerweise sind das:

- **Werbe- und Tracker-Blocker (z.B. uBlock Origin, Adblock Plus, Privacy Badger):** Sie filtern Inhalte heraus, die Werbung oder Tracker enthalten. Damit werden Werbung und viele Tracking-Elemente gar nicht geladen .
- **HTTPS- und Script-Filter:** Add-ons, die automatisch auf verschlüsselte Verbindungen umstellen oder unsichere Scripts unterbinden.
- **Spezial-Tools:** Datenschutz-orientierte Tools, die z. B. Cookies im Hintergrund löschen oder automatisch Anti-Tracking-Listen aktualisieren.

Browser wie Brave zeigen, wie wichtig diese Funktionen sind: Brave hat einen eingebauten Inhalts-Blocker und viele Datenschutz-Funktionen von Haus aus aktiviert. Wer eine Erweiterung wie einen Adblocker nutzt, verhindert, dass viele Tracker überhaupt Zugriff auf die eigenen Daten bekommen. Das erhöht nicht nur den Schutz der Privatsphäre, sondern macht das Surfen meist auch schneller und stromsparender.

Einschränkungen auf iOS

Anders als bei Android gelten auf iOS strenge Regeln: Apple verlangt, dass alle Browser-Apps auf dem iPhone und iPad die WebKit-

Engine (Apples Safari-Modul) zum Rendern von Webseiten verwenden. Unter dieser Haube arbeiten dann auch Browser wie Chrome, Firefox oder iCab auf dem iPhone – technisch sind sie ähnlich wie Safari. Das bedeutet: Neue Engines (z. B. Googles Blink) sind nicht erlaubt, weshalb sich Funktionen stark ähneln. Erst seit iOS 15 können iPhone-User Safari-Erweiterungen aus dem App Store installieren, z. B. Werbeblocker oder Passwort-Manager. Die meisten Drittanbieter-Browser auf iOS haben nur sehr begrenzte Plugin-Unterstützung.

Trotzdem gibt es Ausnahmen: Einige iOS-Browser, allen voran iCab Mobile, bieten eigene Filter- und Werbeblocker-Mechanismen – auch wenn sie WebKit nutzen . iCab kann populäre Filterlisten (EasyList, Adblock Plus, uBlock usw.) direkt nutzen und erlaubt sogar eigene Filterregeln . Das macht iCab zu einer der wenigen iOS-Apps, bei der man ähnlich wie auf dem Desktop Ads und Tracker umfassend blocken kann.

Empfohlene Browser für Android und iOS

Android: Auf Android haben Nutzer die größte Freiheit bei Browser-Erweiterungen. Empfehlenswert sind:

- **Brave (Android):** Ein Chromium-basierter Browser mit integrierter Werbe- und Tracker-Blockade . Brave schützt standardmäßig vor Trackern und bietet umfassende Datenschutzeinstellungen (sog. Brave Shields).
- **Mozilla Firefox (Android):** Bietet ab Werk „Enhanced Tracking Protection“ (Tracking-Schutz ist standardmäßig aktiv) . Seit Ende 2023 gibt es einen neuen Firefox für Android mit offener Erweiterungsunterstützung – Benutzer können endlich die gleichen Add-ons wie auf dem Desktop installieren .

- **Bromite (Android):** Ein modifizierter Chromium-Browser mit eingebautem Adblocker und weiteren Privatsphäre-Verbesserungen. Er ist quelloffen und entfernt Google-spezifische Datensammelmechanismen.
- **Kiwi Browser (Android):** Ein weiterer Chromium-Fork, bekannt dafür, dass man Chrome-Erweiterungen installieren kann (z. B. uBlock Origin). So bekommt man auf Android funktionsreiche Add-ons.
- **DuckDuckGo Privacy Browser (Android):** Einfache, datenschutzorientierte Oberfläche mit Tracker-Blocker und einem „Feuerzeug"-Button, der alle Tabs und Daten sofort löscht. (Erweiterungen unterstützt er nicht; Fokus liegt auf einfacher Handhabung.)

iOS: Wegen Apples WebKit-Zwang gibt es weniger Auswahl, aber trotzdem einige empfehlenswerte Optionen:

- **Safari (iOS):** Apple Safari ist auf iPhone und iPad der Standardbrowser. Seit iOS 15 kann man Safari-Erweiterungen aus dem App Store installieren (etwa Werbeblocker oder Passwortmanager). Zudem hat Safari selbst einen recht einfachen Tracking-Schutz.
- **Mozilla Firefox (iOS):** Wie auf Android bietet Firefox eine solide Basis mit Tracking-Schutz und Privatsphäre-Features. Auch wenn er in WebKit läuft, bringt er vertraute Funktionen und hoffentlich bald auch Web-Extensions nach iOS (ähnlich wie Android) .
- **Brave (iOS):** Die iOS-Version von Brave nutzt ebenfalls WebKit, liefert aber die Brave-typischen Shields (Tracker- und Werbeblock) in der Oberfläche. So profitieren auch iPhone-Nutzer von den bekannten Brave-Funktionen.

- **DuckDuckGo Privacy Browser (iOS):** Auch für iOS verfügbar, bietet er integrierten Tracker-Schutz und ein einfaches Design. (Auf iOS ist das Toolset etwas eingeschränkter, es gibt keinen zusätzlichen Schutz durch App Tracking wie auf Android.)
- **iCab Mobile (iOS):** Speziell hervorzuheben ist iCab Mobile – einer der wenigen iOS-Browser, der eigene Filterlisten/Plug-ins erlaubt. iCab unterstützt u. a. EasyList/AdBlock-Plus-Listen, mit denen Werbung und Tracker effektiv blockiert werden können. Darüber hinaus bietet iCab viele Komfort- und Datenschutzfunktionen.

iCab Mobile: Speziell für iOS mehr Privatsphäre - Mein Favorit seit Jahren

iCab Mobile ist auf iOS eine Ausnahmelösung: Er erlaubt umfangreiche Werbeblocker-Filter und ähnliche Erweiterungen , was nur wenige iPhone-Browser bieten. Praktisch können Nutzer in iCab beliebige Filterlisten (EasyList, uBlock, AdBlock Plus usw.) direkt laden oder eigene Regeln erstellen . So entfernt iCab zuverlässig Werbung und Tracking-Elemente, bevor sie geladen werden.

Zudem ist iCab sehr individuell anpassbar und bietet viele Komfortfunktionen: Es unterstützt Private Tabs (deaktiviert Speicherung von Surf-Daten) , mehrere Profile/Benutzerkonten (z. B. unterschiedliche Lesezeichen und Einstellungen für Familie oder Arbeit), und einen detaillierten Cookie-Manager. Über die integrierten Datenschutz-Einstellungen kann man etwa den gesamten Browserverlauf, alle Cookies oder gespeicherte Passwörter mit einem Klick löschen . Sogar ein Passwortschutz für den Browser selbst sowie ein „Gast-Modus“ für begrenzten Zugriff sind verfügbar.

Zielgruppen: iCab ist ideal für Nutzer, die hohe Kontrolle und Sicherheit schätzen. Fortgeschrittene Anwender, Familien mit einem iPad oder Nutzer, die mit mehreren Profilen arbeiten, werden die flexiblen Einstellungen lieben. Selbst Einsteiger profitieren von den integrierten Werbeblockern und dem starken Datenschutz, ohne sich selbst komplizierte Filterlisten installieren zu müssen. Der Nachteil: iCab ist keine Freeware (rund 3 €), und die vielen Optionen können anfangs etwas überfordern. Dennoch ist es derzeit eine der wenigen iOS-Apps, mit der man tatsächlichen Plug-in- und Filter-Support ähnlich einem Desktop-Browser hat .

Fazit - Moderne mobile Browser bieten inzwischen viele Möglichkeiten, Tracking zu vermeiden und Werbung zu blockieren. Browser mit Erweiterungen oder integrierten Ad-Blockern (wie Brave, Firefox oder iCab) erhöhen die Privatsphäre deutlich. Insbesondere auf iOS lohnt sich ein Blick auf Speziallösungen wie iCab Mobile oder die neuen Safari-Erweiterungen. Wer diese Tools nutzt, surft sicherer, spart Datenvolumen und verbessert gleichzeitig sein Online-Erlebnis.

Empfehlenswerte Quellen

Wikipedia: Webbrowser
https://de.wikipedia.org/wiki/Webbrowser

Wikipedia: Tracking (Web)
https://de.wikipedia.org/wiki/Tracking_(Web)

Electronic Frontier Foundation (EFF): Surveillance Self-Defense – Browser Tracking
https://ssd.eff.org/module/privacy-students

Lagebericht Security 2025 – Stärker und smarter: Das SOC der Zukunft
https://www.splunk.com/de_de/form/state-of-security.html

Brave Browser – Offizielle Webseite
https://brave.com/

iCab Mobile (iOS) – Offizielle Webseite
http://www.icab.de/mobile.html

DuckDuckGo Privacy Browser – Offizielle Webseite
https://duckduckgo.com/app

Mozilla Firefox Mobile – Offizielle Webseite
https://www.mozilla.org/de/firefox/mobile/

Wie Internetwerbung wirklich funktioniert:

Die geheime Arbeit der Werbebroker

Stell dir vor, du surfst im Netz, klickst auf einen harmlosen Artikel über „Die 10 besten Indoorpflanzen gegen schlechte Laune“ – und in dem Moment beginnt hinter den Kulissen ein kleines Datenfeuerwerk: In Bruchteilen von Sekunden wird dein Besuch versteigert. An den Meistbietenden. Live. Und ohne dass du es merkst.

Willkommen in der Welt des Programmatic Advertising – und bei den Werbebrokern, die deine Daten wie auf einem digitalen Flohmarkt weiterreichen.

Wer oder was ist ein Werbebroker?

Ein Broker für Internetwerbung ist im Grunde ein digitaler Zwischenhändler – eine Plattform, die Angebot und Nachfrage auf dem Online-Werbemarkt in Echtzeit zusammenbringt.

- **Angebot**: Werbeflächen auf Webseiten und Apps.
- **Nachfrage**: Firmen, die Werbung schalten wollen – für Turnschuhe, Versicherungen, Eiweißshakes oder E-Book-Abos.
- **Währung**: Deine Daten.

Wie funktioniert das Ganze in der Praxis?

Das Stichwort lautet Real-Time Bidding (RTB) – also: Echtzeit-Auktionen für Werbeplätze. Und das geht so:

1. Du öffnest eine Webseite

Zum Beispiel eine Nachrichtenseite oder ein Kochblog. Noch bevor die Inhalte komplett geladen sind, passiert Folgendes:

2. Dein Besuch wird als Werbefläche angeboten

Die Seite sagt quasi: „Hier ist ein Nutzer – männlich, 34 Jahre, gerade aus Berlin, interessiert sich für Technik, hat zuletzt nach Wanderschuhen gegoogelt. Will jemand Werbung schalten?“

Diese Infos stammen von Tracking-Technologien: Cookies, Fingerprinting, Werbe-IDs deines Smartphones usw.

3. Die Auktion beginnt

In einem Bruchteil einer Sekunde wird dein Profil (anonymisiert, aber sehr genau) an eine Werbebörse weitergeleitet – eine Plattform, die zwischen Webseiten und Werbekunden vermittelt.

4. Werbekunden geben Gebote ab

Z. B. Nike, Adidas und ein Wanderschuh-Start-up. Alle sagen:

„Ich zahle 0,75 € für diesen Nutzer“ oder „1,10 € – ich will diese Zielgruppe unbedingt!“

5. Der Höchstbietende gewinnt – und zeigt dir seine Anzeige

Der Gewinner darf den Werbeplatz „füllen“ – und während du den Artikel über Zimmerpflanzen liest, siehst du plötzlich Wanderschuhe im Angebot. Zufall? Nein. Es war eine datengetriebene Mini-Auktion.

6. Der Broker bekommt seinen Anteil

Der Werbebroker verdient dabei an jeder Transaktion mit – pro Klick, pro Anzeige, pro Verkauf oder pauschal pro 1.000 Sichtkontakte (CPM = Cost Per Mille).

Welche Daten werden gehandelt?

Ein Broker interessiert sich nicht für deinen Namen, sondern für dein Nutzerverhalten:

- Welche Seiten du besuchst.
- Welche Geräte du nutzt.
- Welche Produkte du anschaust.
- Wie lange du dich wo aufhältst.
- Wo du dich befindest (GPS, IP-Adresse).
- Wie alt du wahrscheinlich bist, welches Geschlecht du hast, usw.

Diese Daten sind zwar technisch „pseudonymisiert“, aber in Summe ergibt sich ein sehr genaues Profil von dir. Und das Profil kann für Werbung verkauft werden – wieder und wieder.

Wichtig: Es handelt sich um einen automatisierten Massenhandel Pro Tag finden weltweit Milliarden solcher Auktionen statt.

Das ganze System basiert auf Geschwindigkeit und Präzision. Menschen steuern das nicht mehr – Algorithmen übernehmen den Job. Und das in Millisekunden.

Bekannte Werbebroker & Plattformen

- Google Ads / AdSense (USA) – Marktführer
- Meta Ads (Facebook/Instagram, USA)
- The Trade Desk
- AppNexus / Xandr
- Criteo (Frankreich)
- Taboola / Outbrain (für Native Ads)

Diese Plattformen arbeiten mit Hunderten von Seiten, Shops und Drittanbietern zusammen.

Warum das problematisch sein kann

1. Undurchsichtige Datenspuren

Du weißt oft nicht, wer dich gerade trackt oder dein Profil nutzt. Viele Tracker sind unsichtbar und stammen von Drittanbietern.

2. Datenweitergabe an Dutzende Firmen

Eine Analyse der „Irish Council for Civil Liberties“ zeigte, dass bei einem einzigen Webseitenbesuch deine Daten an hundert oder mehr Firmen weitergereicht werden können.

3. DSGVO-Verstöße & Grauzonen

Gerade in Europa ist vieles davon rechtlich umstritten. Es gibt bereits Klagen gegen Google & Co., weil die Nutzer*innen keine echte Kontrolle über ihre Daten haben.

4. Persönlichkeitsprofile & Manipulation

Wer viele Daten über dich hat, weiß, was dich triggert. Das kann bei politischen Kampagnen, Produktempfehlungen oder sogar in Dating-Apps Einfluss auf dein Verhalten nehmen.

Wie kann man sich schützen?

- Werbeblocker & Trackingblocker (z. B. uBlock Origin, Privacy Badger)
- Cookies regelmäßig löschen
- Browser mit Fokus auf Datenschutz (z. B. Firefox, Brave, DuckDuckGo)
- VPN verwenden – erschwert das Nachverfolgen durch IP-Adressen
- Privates Surfen / Inkognito-Modus
- Tools wie „NoScript“ oder „Consent-O-Matic“

Fazit - Deine Daten sind wertvoll – und heiß gehandelt! Die Welt der digitalen Werbung ist ein gigantischer, unsichtbarer Marktplatz, auf dem dein Verhalten zur Währung geworden ist. Und Broker sind die cleveren Mittelsmänner, die aus deinem Klick bares Geld machen.

Es ist also nicht übertrieben zu sagen:
„Wenn du nichts für ein Produkt bezahlst – bist du selbst das Produkt.“

Empfehlenswerte Quellen

Wikipedia: Real-Time Bidding (RTB)
https://en.wikipedia.org/wiki/Real-time_bidding

Wikipedia: Programmatic Advertising
https://en.wikipedia.org/wiki/Programmatic_advertising

Cybersicherheit Europa 2025: Netskope Threat Labs Report deckt alarmierende Trends auf
https://digital-magazin.de/report-cybersicherheit-europa-2025/

The Trade Desk – Offizielle Webseite
https://www.thetradedesk.com/

How Do Google Ads Work? (Easy Guide for Beginners)
https://www.reliablesoft.net/what-is-google-ads/

bit.ly/was-zur-Hölle?

Warum URL-Shortener praktisch sind – und gleichzeitig ein Albtraum für deine Online-Sicherheit

Kurz gesagt: Was ist ein URL-Shortener?

Ein URL-Shortener ist so etwas wie ein Zauberstab für super lange Webadressen, die man nicht abtippen möchte.

Statt eines Links wie:

https://www.supergeheimerdienst.de/berichte/topsecret/2025/mai/bericht_xyz_version_final_final2.pdf

gibt's dann:

bit.ly/3xR4YzG

Voilà! Aufgeräumt. Kompakt. Klickfreundlich.

Solche Dienste (z. B. bit.ly, tinyurl.com, t.co, goo.gl, ow.ly) nehmen lange URLs und geben dir eine kurze – perfekt für Twitter, Visitenkarten oder Plakate, auf denen einfach kein Platz für ein Slash-Gewitter ist.

Der Nutzen – oder: Warum jeder sie liebt

1. Platzsparer:

Vor allem bei Social Media, wo Zeichen begrenzt sind (Twitter, ich sehe dich), sind kurze URLs Gold wert.

2. Statistik-Fans werden glücklich:

Wer einen eigenen Shortlink erzeugt, kann oft sehen, wie viele Leute draufgeklickt haben, aus welchem Land, mit welchem Gerät – quasi Google Analytics in Light-Version.

3. Branding:

Manche Unternehmen nutzen eigene Shortener wie nyt.ms (New York Times) oder amzn.to (Amazon), um professionell und vertrauenswürdig aufzutreten.

4. Übersichtlicher Look:

Ein kurzer Link wirkt harmlos, fast niedlich. Er sagt: "Hey, klick mich, ich beiße nicht!" (Spoiler: Manche beißen doch.)

Die dunkle Seite: Warum sie ein Sicherheitsrisiko sind

1. Du weißt nicht, wohin du klickst

Das größte Problem: Ein verkürzter Link ist wie eine mysteriöse Schachtel. Du weißt nicht, was drin ist, bis du klickst.

Ein niedlicher Link wie bit.ly/2C4HjK9 kann auf alles verweisen:

- Eine harmlose Katzen-GIF-Seite.
- Oder eine Phishing-Seite, die aussieht wie dein Onlinebanking.
- Oder ein Exploit (ein digitaler Dietrich), der deinem Gerät eine Schwachstelle ausnutzt und dann das Fürchten lehrt.

2. Ideal für Phishing & Malware

Angreifer nutzen Shortener gezielt, um bösartige Seiten zu verschleiern. Besonders perfide: Bei E-Mails oder Social-Media-

Beiträgen wirkt der kurze Link neutral, da man die Zieladresse ja nicht erkennen kann.

3. Manipulierbar in Werbung und Spam

Ein Werbetreibender kann dir einen Shortlink geben, der zuerst zu einem harmlosen Inhalt führt – und später geändert wird, um dich auf eine ganz andere Seite zu leiten. Der Link bleibt gleich, aber das Ziel wird ausgetauscht.

4. Keine Kontrolle beim Klicken

Wenn du einem Shortlink vertraust, vertraust du gleichzeitig dem Anbieter (z. B. bit.ly). Fällt dieser Dienst aus, gehackt oder verkauft, kann jeder Link umgeleitet oder missbraucht werden.

Wie erkennt man einen URL-Shortener?

Die meisten Shortener erkennst du direkt an der Domain:

- bit.ly, tinyurl.com, t.co, is.gd, ow.ly, rebrand.ly
- amzn.to, fb.me, youtu.be, nyt.ms (eigene Shortener großer Dienste)

Wenn dir ein Link verdächtig kurz vorkommt oder aus Zahlen und Buchstaben besteht, wie:

bit.ly/3JxG2eX
t.co/Xz9fLmP

... solltest du skeptisch werden.

Tools, um Shortlinks zu entschlüsseln

Zum Glück gibt’s auch digitale Taschenlampen für diese dunklen Ecken des Webs. Du kannst einen Shortlink “entkürzen”, bevor du draufklickst:

Online-Tools:

- https://checkshorturl.com
  Zeigt dir die Originaladresse und scannt sie sogar auf Gefahren.
- https://unshorten.me
  Einfache Oberfläche, zeigt dir das Ziel samt Sicherheitseinschätzung.
- https://getlinkinfo.com
  Liefert Meta-Informationen zur Zielseite.

Browser-Add-ons:

- Unshorten.link (für Firefox & Chrome)
  Verhindert automatisch das direkte Öffnen von Shortlinks und zeigt stattdessen die Zieladresse.
- LinkPeelr
  Entpackt gekürzte Links auf Knopfdruck.

Fazit - Vertrauen ist gut, Vorschau ist besser

URL-Shortener sind praktische Helferlein im digitalen Alltag – aber sie haben einen Haken: Du siehst nicht, wohin du gehst. Und in Zeiten von Fake-Shops, Phishing-Mails und Drive-by-Malware kann das eine Einladung zur digitalen Bauchlandung sein.

Merke dir die goldene Regel:

Klicke nie auf einen Link, den du nicht sehen kannst.

Nutze Tools, Browser-Add-ons oder schlicht deinen Verstand. Und wenn dir jemand per E-Mail „bit.ly/deine-geheime-rückzahlung“ schickt, frag dich:

Warum sollte eine seriöse Bank einen Link verwenden, der klingt wie ein Passwort eines paranoiden IT-Admins (ow.ly/PW4Good1s)?

Und: Es kann nicht schaden dein Smartphone (ja auch deinen Rechner) immer mit den neusten Updates zu versorgen! Macht man dies nicht, lässt man gegebenenfalls Türen für Hacker offen, oder vereinfacht dem Hacker die Nutzung eines sogenannten Exploits (der digitale Dietrich für die digitale Eingangstür zum Smartphone, oder dem Rechner).

Empfehlenswerte Quellen

Wikipedia URL-Shortener
https://de.wikipedia.org/wiki/URL-Shortener

Erweitern und überprüfen Sie alle Ihre verkürzten Links
https://checkshorturl.com

Unshorten.me ist ein kostenloser Service zum Entkürzen von URLs, die von URL-Verkürzungsdiensten erstellt wurden
https://unshorten.me

Wikipedia Exploits
https://de.wikipedia.org/wiki/Exploit

Sind Werbeblocker im Browser legal?

Werbeblocker (auch Adblocker genannt) sind Programme oder Erweiterungen für den Browser, die Werbung auf Internetseiten blockieren. Sie verhindern, dass Banner, Pop-ups oder Videowerbung angezeigt werden . Technisch funktioniert das meist über Filterlisten: Der Adblocker erkennt anhand der Webadresse oder von Code-Mustern, dass es sich um Werbung handelt, und unterdrückt das Laden dieser Inhalte. Für den Nutzer bedeutet das schnellere Ladezeiten der Seiten und einen geringeren Datenverbrauch, weil weniger Drittinhalte geladen werden.

Viele Menschen nutzen Werbeblocker, weil Online-Werbung oft als lästig empfunden wird. Häufige Gründe sind:

- **Störende Pop-ups und Videowerbung:** Werbung unterbricht beim Surfen den Lesefluss (z.B. aufdringliche Pop-up-Fenster oder Werbebanner).
- **Schnellere Webseiten:** Da Adblocker Anzeigen ausblenden, laden Webseiten oft schneller.
- **Datenschutz:** Werbung trackt oft das Nutzerverhalten. Mit Werbeblockern werden Tracker und Cookies von Werbenetzwerken verhindert, was die Privatsphäre schützt.
- **Hohe Verbreitung:** In Deutschland setzen etwa 25 % der Internetnutzer Adblocker ein , vor allem auf mobilen Geräten.

Damit nutzen in etwa jeder vierte Deutsche einen Werbeblocker . Die Nutzung schwankt je nach Land und Altersgruppe, ist aber global weit verbreitet.

Sind Werbeblocker in Deutschland erlaubt?

In Deutschland ist die Nutzung von Werbeblockern grundsätzlich legal. Das sagen Gerichte und Experten unmissverständlich. So entschied der Bundesgerichtshof (BGH) 2018 in einem Verfahren, dass das verbreitete Programm Adblock Plus keine unzulässige Handlung darstellt . Der BGH erklärte, der Einsatz eines solchen Werbeblockers sei "zulässig" und nicht wettbewerbswidrig . In der Urteilsbegründung hieß es unter anderem, dass die Nutzer den Filter selbst installieren müssen. Da sie freiwillig entscheiden, welchen Inhalt sie angezeigt bekommen, liegt kein unzulässiger Eingriff vor . Der Verlag (hier Axel Springer) könne anderenfalls ja einfach seinen Dienst für Adblocker-Nutzer sperren, wenn er wollte .

Auch frühere Gerichtsentscheidungen waren bereits zu Gunsten der Adblocker gefallen. So hatte das Landgericht Hamburg 2017 im Verfahren gegen Adblock Plus erklärt, das Programm ändere nur die Darstellung der Webseite, nicht aber deren eigentlichen Programmcode . Eine Verletzung des Urheberrechts liege daher nicht vor . Und auch kartell- und wettbewerbsrechtliche Klagen gegen Werbeblocker wurden zurückgewiesen . Zusammengefasst: Nach deutschem Recht dürfen Nutzer selbst bestimmen, ob sie Werbung auf ihrem Bildschirm sehen. Solange keine technischen Sperren umgangen werden, verstoßen Werbeblocker nicht gegen Gesetze .

Rechtliche Lage in Österreich und der Schweiz

In Österreich und der Schweiz ist die Lage ähnlich: Es gibt kein Verbot gegen die Nutzung von Werbeblockern. Nach Einschätzung von

Rechtsexperten hängt vieles davon ab, dass der Nutzer die Wahl hat. Im österreichischen Wettbewerbsrecht wird betont, dass der User selbst entscheidet, wie viel Werbung er blockiert . Solange der Nutzer also selbst festlegt, welche Anzeigen er ausblendet (zum Beispiel indem er einen Filter aktiviert), gilt dies nicht als unlautere Beeinträchtigung. Ein komplett automatisches Entfernen aller Werbung ohne Einfluss des Nutzers wäre eher problematisch. Praktisch bedeutet das: Auch in Österreich kann man Werbeblocker benutzen, ohne gegen geltendes Recht zu verstoßen . (2013 hat der ORF eine Prüfung durch die Wettbewerbsbehörde angeregt, doch grundsätzliche Verbote existieren bisher nicht.)

In der Schweiz gibt es bislang keine oberste Gerichtsentscheidung zu Adblockern. Experten der Wettbewerbsrechtspraxis bewerten Adblocker jedoch ähnlich wie in Deutschland: Werbeblocker wie Adblock Plus gelten grundsätzlich als zulässig nach heutigem Schweizer Recht . Entscheidend ist, dass der Nutzer transparent erfährt, wie die Filter funktionieren, und dass er selbst die Kontrolle behält . Solange Webseiten nicht von oben herab bestimmte Werbung bevorzugen oder löschen (zum Beispiel über Whitelists bei Bezahlsystemen), sehen Fachleute keine klare Rechtswidrigkeit . Zusammengefasst lässt sich sagen: Auch in Österreich und der Schweiz besteht kein strafrechtliches Verbot gegen Werbeblocker .

EU-weit

Auch auf EU-Ebene existiert kein Verbot, Adblocker zu nutzen. Es gibt keine EU-Richtlinie, die das Blockieren von Online-Werbung explizit untersagt. Im Gegenteil: Datenschutz und Nutzerrechte werden in der EU aktuell eher gestärkt. So schreibt etwa die ePrivacy-Richtlinie, dass Online-Dienste die Zustimmung der Nutzer einholen müssen, bevor Daten zu Werbezwecken verarbeitet werden. Datenschutzbehörden mahnen deshalb, dass manche Methoden zum Erkennen von

Werbeblockern (wie etwa bei YouTube) gegen diese Datenschutzregeln verstoßen könnten . In einem aktuellen Fall kritisierten EU-Datenschützer, dass YouTube Programme einsetzt, um Adblocker zu erkennen, und dabei gegen die EU-Datenschutzregeln verstößt . Das zeigt: EU-weit hat der Datenschutz Vorrang. Werbeblocker an sich werden nicht verboten – im Gegenteil fördern sie teils ja den Schutz der Privatsphäre. Ein Nutzer befindet sich also rechtlich auf der sicheren Seite, wenn er Werbung blockiert. Webseitenbetreiber können allerdings in ihren Nutzungsbedingungen verlangen, Adblocker abzuschalten, oder per Skript den Zugriff einschränken.

Sind Werbeblocker in den USA legal?

In den USA ist die Situation ähnlich wie in Europa. Grundsätzlich ist es hier erlaubt, Werbung zu blockieren. Mehrere US-Gerichte haben das Recht der Nutzer bestätigt, selbst zu bestimmen, welche Inhalte oder Anfragen auf ihren eigenen Geräten angezeigt werden . Oder wie es in einem US-Blog zusammengefasst wurde: Man hat als Internetnutzer das Recht, selbst zu filtern .

Allerdings gibt es in den USA mit dem Digital Millennium Copyright Act (DMCA) eine Bestimmung, die das Umgehen technischer Schutzmaßnahmen verbietet. Das heißt: Nutzt eine Website aktiv Anti-Adblock-Technik (etwa ein Skript, das Besucher mit Adblocker automatisch blockiert), und ein Nutzer umgeht diese Maßnahme durch den Adblocker, könnte das ein Problem nach dem DMCA sein . Kurz gesagt: Werbung zu blockieren ist selbst nicht illegal, aber das gezielte Umgehen von Sperrmaßnahmen kann gegen das Urheberrecht verstoßen . Solange man also einfach nur Werbung auf den Seiten entfernt, gibt es rechtlich keine Schwierigkeiten . Erst wenn man gezielt gegen Anti-Blocker-Systeme vorgeht, wird es problematisch.

Zusammengefasst: Ob in Deutschland, der EU oder den USA – das einfache Blockieren von Werbung ist nicht verboten. Nutzer dürfen entscheiden, was auf ihrem Bildschirm erscheint . Es gibt derzeit kein Gesetz, das Privatpersonen wegen der Verwendung eines Adblockers bestraft.

Konflikt zwischen Nutzern und Website-Betreibern

Trotz der rechtlichen Erlaubnis führt die Verwendung von Werbeblockern immer wieder zu Streit. Viele Website-Betreiber – vor allem Nachrichtenportale und Medienseiten – finanzieren sich durch Werbeeinnahmen. Sie argumentieren, dass Adblocker ihnen Geld entziehen und ihr Geschäftsmodell gefährden. Daher setzen einige von ihnen Gegenmaßnahmen ein. Technik-Tricks erkennen aktiv, ob ein Besucher einen Adblocker nutzt. Ist der Blocker eingeschaltet, fordern manche Seiten den Nutzer auf, ihn auszuschalten, oder geben Inhalte nur dann frei, wenn Werbung geschaltet wird . In Extremfällen sperren Angebote Besucher mit Adblocker komplett aus.

Ein bekanntes Beispiel ist YouTube: Google verbietet offiziell den Einsatz von Adblockern auf dem Videoportal. Wer dennoch Werbung blockt, kann laut Nutzungsbedingungen sein Konto verlieren. In Deutschland haben Datenschützer allerdings kritisiert, dass die Erkennung von Adblockern durch YouTube gegen EU-Datenschutzvorgaben verstoße . Auch YouTube-Nutzer berichten gelegentlich, dass ihre Accounts gesperrt wurden, weil sie Adblocker verwendet hatten . Andere Dienste – etwa Online-Magazine – setzen auf freundliche Ansagen oder Paywalls als Kompromiss: Entweder schaltet der Nutzer Werbung zu oder er zahlt für werbefreie Inhalte direkt.

Für Nutzer droht dabei keine rechtliche Strafe. Niemand muss befürchten, wegen der Verwendung eines Werbeblockers verklagt oder belangt zu werden. Wie gesagt, das Blockieren ist legal . Die einzige

Konsequenz ist meist, dass man auf bestimmten Webseiten ohne Werbung möglicherweise nicht mehr weiterkommt. Wer sich strikt weigert, Werbung zu akzeptieren, kann von manchen Angeboten ausgesperrt oder zu einem Abonnement gedrängt werden. Diese Einschränkungen sind jedoch technischer Natur – eine Verletzung des Gesetzes ist damit nicht verbunden .

Fazit - Kurzum: Werbeblocker zu nutzen ist legal. In Deutschland wie international gibt es kein Verbot, Anzeigen auf dem eigenen Computer oder Smartphone zu filtern . Nutzer dürfen im Internet selbst entscheiden, welche Inhalte sie sehen und welchen nicht. Allerdings stehen viele Content-Anbieter hinter der Paywall-Werbung, weshalb es immer wieder Streit um Werbeeinnahmen gibt. Webseiten reagieren mit Aufforderungen zum Deaktivieren von Blockern, Sperren oder alternativen Finanzierungsmodellen. Rechtlich gilt aber klar: Werbeblocker sind kein Straftatbestand, sondern erlaubte Software. Nutzer sollten nur darauf achten, dass sie keine Gesetze umgehen (also etwa keine fiese Anti-Adblock-Sperre hacken) . Solange man das berücksichtigt, ist man auf der sicheren Seite – rechtlich wie technisch.

Empfehlenswerte Quellen

Wikipedia: Adblocker
https://de.wikipedia.org/wiki/Adblocker

Bundesgerichtshof (BGH) 2018: Urteil zu Adblock Plus
https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2018/2018048.html

Adblocker im Internet: Sind die Werbeblocker legal? Das müsst ihr beachten...
https://www.netzwelt.de/adblocker/index.html

Sind Adblocker legal?
https://www.agentur-braun.de/sind-adblocker-legal/

ePrivacy-Richtlinie der EU (2002/58/EG)
https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32002L0058

Electronic Frontier Foundation (EFF): Thema Add Blocking
https://www.eff.org/search/site/add%20blocking

Werbung und Tracker zu Hause blockieren:

So schützt du dein Heimnetzwerk mit eigenen Geräten

Im Internet sind wir ständig von Werbung und unsichtbaren Trackern umgeben, die unser Verhalten aufzeichnen, Bewegungsprofile erstellen und uns gezielt beeinflussen wollen. Was viele nicht wissen: Du kannst dein ganzes Heimnetzwerk so konfigurieren, dass diese Werbung und Tracker automatisch blockiert werden – auf allen Geräten, ohne dass du überall separate Apps installieren musst.

In diesem Artikel erklären wir dir, wie du mit externen Geräten dein Zuhause sicherer und werbefrei machst, welche Lösungen es gibt, welche Vor- und Nachteile sie haben und wie viel technisches Wissen du dafür brauchst.

Warum lohnt sich der Schutz im Heimnetzwerk?

Wenn du dein Netzwerk zentral schützt, bekommst du viele Vorteile:

- **Werbefreiheit auf allen Geräten:** Du brauchst keine Adblocker mehr auf jedem einzelnen Gerät – sogar dein Smart-TV oder deine Spielkonsole profitieren davon.
- **Schutz der Privatsphäre:** Tracker und Datensammler (wie Google Analytics, Facebook Pixel etc.) werden blockiert, bevor sie überhaupt Daten absaugen können.
- **Schnelleres Internet:** Werbung und Tracking-Skripte verlangsamen Webseiten – ohne sie lädt vieles schneller.

- **Weniger Datenverbrauch:** Besonders bei mobilen Tarifen oder kleinen DSL-Leitungen zählt jedes Byte.

So funktioniert's: Werbeblocker im Netzwerk

Um Werbung und Tracking im ganzen Heimnetzwerk zu blockieren, brauchst du ein Gerät, das den Internetverkehr filtert. Dieses Gerät steht zwischen deinem Router und dem Internet (oder arbeitet als DNS-Server) und erkennt verdächtige Werbe- und Tracker-Domains – und blockiert sie.

Je nach Gerät oder Methode funktioniert das über:

- DNS-Filter (wie bei Pi-hole)
- lokale Firewalls mit Filterregeln
- VPN-Tunnel mit integriertem Schutz
- oder spezialisierte Plug-&-Play-Lösungen

Lösungen im Überblick

Hier sind einige beliebte Methoden, um dein Heimnetz zu schützen – vom Bastlerprojekt bis zur Plug-&-Play-Box:

1. Pi-hole: Die beliebteste Open-Source-Lösung

Was ist das?

Pi-hole ist eine kostenlose Software, die auf einem kleinen Rechner wie dem Raspberry Pi läuft. Es fungiert als DNS-Server, filtert also Werbung und Tracker, bevor sie deine Geräte erreichen.

Vorteile:

- Kostenlos und Open Source
- Blockiert Werbung netzwerkweit
- Anpassbar (eigene Filterlisten möglich)
- Schöne Weboberfläche zur Verwaltung

Nachteile:

- Keine VPN-Funktion eingebaut.
- Einrichtung kann für Einsteiger anspruchsvoll sein.
- Muss gepflegt und geupdatet werden.

Know-how nötig?

Grundkenntnisse in Netzwerken und etwas technisches Interesse sind hilfreich. Mit Online-Anleitungen und ein wenig Geduld ist es aber machbar – viele Leute lernen dabei auch viel dazu.

2. eBlocker (nicht mehr offiziell erhältlich, aber als DIY möglich)

Was ist das?

eBlocker war ein deutsches Gerät mit benutzerfreundlicher Oberfläche. Es bot Adblocking, Tracking-Schutz und sogar anonyme Surfoptionen per Tor oder VPN. Die Herstellung wurde leider eingestellt, aber die Software kann zum Beispiel noch auf einem Raspberry Pi installiert werden und wird von einer Community weiter gepflegt.

Vorteile:

- Einfache Benutzeroberfläche
- Verschiedene Schutzfunktionen integriert
- Kein Eingriff in einzelne Geräte nötig

Nachteile:

- Nicht mehr offiziell gepflegt
- Einrichtung komplexer als Pi-hole

Know-how nötig?

Für die DIY-Version brauchst du technisches Verständnis und Geduld, um die Software auf einem Raspberry Pi korrekt zu installieren.

3. GL.iNet-Router mit AdGuard Home oder VPN

Was ist das?

GL.iNet bietet kleine Router an, die man hinter seinen Internet-Router klemmen kann. Viele Modelle lassen sich mit OpenWRT, AdGuard Home oder einem VPN-Dienst konfigurieren.

Vorteile:

- Kompakt und transportabel
- VPN- und Adblocking gleichzeitig möglich
- Webinterface zur Steuerung

Nachteile:

- Einrichtung nicht ganz selbsterklärend
- VPN oft langsamer als direkte Verbindung

Know-how nötig?

Wer sich etwas mit Router-Interfaces auskennt, kommt klar. Für Laien ist es möglich, aber mit etwas Einarbeitungszeit.

4. Firewalla, Winston Privacy & Co. – Plug-&-Play-Lösungen

Was ist das?

Kommerzielle Geräte wie Firewalla oder das inzwischen eingestellte Winston Privacy versprechen Schutz ohne Basteln. Einfach anschließen und die App nutzen – fertig.

Vorteile:

- Einfache Einrichtung
- Automatische Updates
- App für Kontrolle & Ausnahmen

Nachteile:

- Kosten (100–200 €)
- Manchmal Abo-Modell
- Weniger individuell anpassbar

Know-how nötig?

Sehr gering – fast jeder kann sie einrichten. Ideal für Menschen, die sich nicht mit Netzwerktechnik befassen wollen.

Wo wird das Gerät installiert?

Fast alle Lösungen werden wie folgt eingerichtet:

- Gerät wird ins Heimnetzwerk eingebunden, oft per LAN-Kabel an den Router.
- Geräte im Netzwerk werden auf den neuen DNS-Server umgestellt (entweder manuell oder über den Router).
- Optionale VPN-Verbindung wird eingerichtet, wenn das Gerät das unterstützt.

Tipp: Wer keinen Zugriff auf den Router hat (z. B. bei Mietroutern), kann auch ein zweites Netzwerk mit dem Schutzgerät als „Zwischen-Router" erstellen.

Was kann schiefgehen?

Nichts ist perfekt – auch diese Lösungen haben ihre Grenzen:

Manche Seiten (z. B. YouTube oder Nachrichtenportale) funktionieren nicht richtig, wenn zu viel geblockt wird.

- Webseiten könnten Inhalte verweigern, wenn sie merken, dass Werbung blockiert wird.
- Wenn du viele Filter aktivierst, kann das Surfen langsamer oder instabil werden.
- Man muss regelmäßig Updates machen, vor allem bei Open-Source-Projekten.

Fazit - Lohnt sich der Schutz zu Hause?

Ja – besonders, wenn du Wert auf Datenschutz, Geschwindigkeit und ein ruhigeres Internet legst. Ein zentrales System zur Werbe- und Tracker-Blockierung ist ein mächtiges Werkzeug – besonders in Haushalten mit mehreren Geräten, Kindern oder smarten Geräten (die oft „nach Hause telefonieren“).

Für Technikinteressierte ist Pi-hole ein hervorragender Einstieg. Wer Komfort sucht, ist mit Geräten wie Firewalla oder GL.iNet-Routern gut beraten. Und wer komplett DIY will, kann sich mit Raspberry Pi und AdGuard Home ein eigenes Filterzentrum bauen.

Ob Anfänger oder Fortgeschrittener – es gibt für jedes Niveau eine passende Lösung. Und sobald du den Unterschied einmal erlebt hast, willst du wahrscheinlich nie wieder ohne Netzwerkschutz surfen.

Empfehlenswerte Quellen

Wikipedia: Pi-hole
https://de.wikipedia.org/wiki/Pi-hole

Offizielle Webseite: Pi-hole
https://pi-hole.net/

AdGuard Home – Offizielle Webseite
https://adguard.com/en/adguard-home/overview.html

GL.iNet Router – Offizielle Webseite
https://www.gl-inet.com/

Firewalla – Offizielle Webseite
https://firewalla.com/

Werbung und Tracking blockieren: Empfehlenswerte Filterlisten
https://www.kuketz-blog.de/werbung-und-tracking-empfehlenswerte-filterlisten/

Tarnen des Browsers

Wie du beim Online-Shopping bares Geld sparen kannst

Das Internet weiß mehr über dich, als dir lieb ist. Dein Browser plaudert bei jedem Besuch einer Webseite fleißig aus dem Nähkästchen: Welches Gerät du benutzt, welches Betriebssystem läuft, woher du kommst – sogar, ob du gerade ein teurer Apple-Nutzer oder ein bodenständiger Android-Fan bist.

Das Problem dabei: Diese Informationen beeinflussen nicht nur, welche Werbung du siehst, sondern auch, wie viel du im Online-Shop bezahlst. Richtig gelesen: Manchmal ist es wirklich teurer, ein schickes MacBook zu besitzen – zumindest aus Sicht des Webshops.

Aber keine Sorge: Wer ein bisschen trickst und seinen Browser tarnt, kann beim Einkaufen echtes Geld sparen. Wie das geht und welche Tools dir helfen, erfährst du hier.

Warum Apple-Nutzer oft mehr bezahlen müssen?

Mehrere Studien haben gezeigt, dass Online-Shops – besonders Reiseportale – die Preise abhängig vom verwendeten Gerät anpassen. Besonders Apple-Nutzer gelten als kaufkräftiger. Schließlich: Wer 1.500 Euro für ein iPhone auf den Tisch legt, der hat vermutlich auch 50 Euro mehr für ein Hotelzimmer übrig, oder?

Zum Beispiel zeigte das Reiseportal Orbitz Mac-Usern gezielt teurere oder luxuriösere Hotels an als Windows-Nutzern. Die Technik dahinter ist simpel: Dein Browser verrät mit dem sogenannten User-Agent, welches Gerät du benutzt.

Dazu kommt noch der Referrer – eine Infozeile, die übermittelt, von welcher Webseite du gerade kommst. Warst du auf einer teuren Vergleichsseite unterwegs? Prima, dann zeig dir der Shop gleich die Premium-Angebote.

Was dein Browser alles über dich verrät

Wenn du eine Webseite aufrufst, sendet dein Browser automatisch:

- User-Agent: “Hallo, ich bin ein iPhone 14 Pro mit Safari!”
- Referrer: “Und ich komme gerade von einer Luxusreiseplattform.”
- Weitere Infos: Bildschirmgröße, Sprachversion, installierte Plugins etc.

Zusammen ergibt das ein hübsches Nutzerprofil – perfekt, um Preise und Angebote auf deine (vermutete) Zahlungsbereitschaft zuzuschneiden.

So kannst du deinen Browser tarnen

Jetzt wird’s spannend: Mit ein paar einfachen Tricks kannst du verhindern, dass Shops diese Daten gegen dich verwenden.

1. User-Agent fälschen

Der User-Agent ist eine Art Visitenkarte deines Browsers. Indem du ihn änderst, kannst du dich als Android-Handy, Windows-PC oder sogar als Googlebot ausgeben.

Beliebte Tools dafür:

- User-Agent Switcher for Chrome (für Chrome)
- User-Agent Switcher and Manager (für Firefox)
- ModHeader (Chrome, Firefox, Edge) – Profi-Tool zum gezielten Anpassen von Header

Damit kannst du zum Beispiel behaupten: „Nein, ich bin kein teurer Mac-User, ich bin ein günstiges Android-Handy!“

2. Referrer manipulieren oder verbergen

Der Referrer zeigt an, von welcher Seite du kommst. Auch hier kannst du tricksen.

Praktische Erweiterungen:

- Referer Control (für Chrome und Firefox)
- Smart Referer (für Firefox)
- ModHeader (für alle großen Browser)

Diese Tools verhindern, dass Shops wissen, ob du von einer Vergleichsseite, einem Gutscheinportal oder einer Luxusreiseplattform kommst. Ohne Referrer sehen sie dich nur als “neutralen” Besucher – oft mit besseren Preisen.

3. Privatmodus verwenden

Im Inkognito-Modus (Chrome) oder Privaten Modus (Firefox, Safari) werden Cookies und Cache nicht gespeichert. Das hilft, personalisierte Preisanpassungen zu umgehen. Manche Shops erhöhen die Preise nämlich gezielt, wenn sie merken: „Aha, der war schon dreimal da, der will das Zimmer unbedingt!“

Tipps für noch mehr Tarnung:

- Cookies regelmäßig löschen oder per Browser-Einstellung automatisch nach jeder Sitzung entfernen.
- VPN nutzen, um deinen Standort zu verbergen (manchmal gibt es in anderen Ländern günstigere Angebote).
- Mehrere Browser testen: Mal im mobilen Browser einkaufen, mal als Windows-User auftreten – manchmal gibt es überraschende Unterschiede!

iOS-Nutzer: Tarnen auf dem iPhone

Auch auf dem iPhone gibt es Möglichkeiten, sich zu tarnen:

- iCab Mobile: Flexibler Browser mit integriertem User-Agent-Wechsler und Referrer-Schutz.
- Aloha Browser: Einfach zu bedienen, VPN inklusive und User-Agent-Switcher verfügbar.
- Onion Browser: Wer auf maximale Anonymität Wert legt, surft hier über das Tor-Netzwerk.

In Safari auf iOS kannst du zumindest über „Desktop-Website anfordern" minimal den User-Agent beeinflussen – ein kleiner Trick, der manchmal reicht.

Fazit - Dein Browser ist wie ein Plaudertaschen-Assistent, der ohne Tarnung jedem Verkäufer zuruft: „Er hier! Er zahlt bestimmt mehr!"

Mit ein paar kleinen Handgriffen kannst du ihn zum diskreten Butler machen, der deine Identität geheim hält – und dir damit beim Online-Shopping bares Geld spart.

Also: User-Agent wechseln, Referrer verstecken, Cookies löschen – und mit etwas Glück buchst du deinen nächsten Flug günstiger als dein Sitznachbar im Flugzeug.

Empfehlenswert Quellen

Wikipedia: HTTP-Referer
https://de.wikipedia.org/wiki/HTTP-Referer

Wikipedia: Device Fingerprinting
https://en.wikipedia.org/wiki/Device_fingerprint

Electronic Frontier Foundation (EFF): Panopticlick
https://panopticlick.eff.org/

Tools zur Tarnung des Referrers und User-Agents:

uBlock Origin (Browser-Erweiterung)
https://ublockorigin.com/

Privacy Badger (Browser-Erweiterung)
https://privacybadger.org/

Vorsicht, Falle!

Wie du Fake-Shops erkennst, bevor sie dein Konto plündern

Kennst du das? Du scrollst durch Social Media oder suchst spontan nach einem günstigen Paar Sneaker – und bam, da ist er: Der perfekte Shop. Riesige Auswahl, Preise zum Dahinschmelzen, sogar deine Lieblingsmarke ist dabei! Alles wirkt wie im echten Leben – nur dass es diesen „Shop" gar nicht gibt.

Willkommen in der Welt der Fake-Shops – digitalen Mogelpackungen, die dich um dein Geld bringen wollen, ohne jemals Ware zu liefern.

Was ist ein Fake-Shop eigentlich?

Ein Fake-Shop ist eine betrügerische Online-Verkaufsseite. Er sieht aus wie ein ganz normaler Onlineshop, bietet oft Markenprodukte zu stark reduzierten Preisen an – aber der ganze Shop ist nur eine Attrappe.

- Du gibst deine Daten ein.
- Du bezahlst.
- Und wartest… und wartest… und wartest…
- …auf ein Paket, das niemals kommt.

In manchen Fällen kommt sogar eine Lieferung – aber mit billigem Plunder aus Fernost, der mit dem beworbenen Produkt nichts zu tun hat. Oder es kommt eine Mail mit dem Satz: „Sorry, ausverkauft – Rückzahlung leider nicht möglich."

Warum sind Fake-Shops so gefährlich?

Weil sie:

- dein Geld klauen
- deine Daten abgreifen (z. B. Adresse, Kreditkartennummer, E-Mail)
- dein Vertrauen in den Onlinehandel erschüttern
- manchmal sogar deine Daten weiterverkaufen
- Und das Gemeine: Viele dieser Shops sehen auf den ersten Blick richtig professionell aus – mit schönem Layout, Warenkorb, Gütesiegel (meist gefälscht) und allem drum und dran.

Wie erkennst du einen Fake-Shop?

Die 10 wichtigsten Warnzeichen:

1. Preise, die „zu gut" sind

Wenn ein iPhone für 199 € oder Nike-Schuhe für 30 € angeboten werden: Alarmstufe Rot! Kein echter Händler verkauft solche Produkte so günstig – außer bei versteckten Kosten oder im Fantasieland.

2. Nur Vorkasse, kein PayPal oder Rechnung

Fake-Shops bieten meist nur unsichere Zahlungsmethoden wie Vorkasse oder Kreditkartenzahlung an.

Sichere Shops bieten immer:

- PayPal

- Rechnungskauf
- Klarna
- Lastschrift

Merke Dir einfach: Fake-Shops meiden diese – weil sie dich nicht rückbuchen lassen wollen.

3. Fehlendes Impressum oder dubiose Angaben

Kein Impressum? Nur eine komische Gmail-Adresse als Kontakt? Eine angebliche Firma in Litauen ohne Steuernummer?

Achtung: In Deutschland ist ein Impressum gesetzlich Pflicht.

4. Viele Rechtschreibfehler

Wenn die Seite klingt, als hätte jemand Google Translate benutzt oder gerade das Abi in Deutsch abgebrochen hat, ist das ein Hinweis. Echte Shops investieren in Texte, die vertrauenserweckend sind.

5. Keine oder gefälschte Bewertungen

Wenn alle Bewertungen 5 Sterne haben und klingen wie von Robotern geschrieben – „Ich bin so begeistert und kaufe wieder" – dann solltest du misstrauisch sein. Auch Gütesiegel wie „Trusted Shops", „TÜV-geprüft" oder „Verbraucherschutz.de" können gefälscht sein.

6. Neue oder obskure Domainnamen

Wenn der Shop unter www.markenschuhe-online-deals24.xyz läuft oder du eine Seite mit ungewöhnlicher Domainendung wie .top, .store, .club hast, sei vorsichtig.

7. Kurzes Bestehen der Webseite

Mit einem Whois-Dienst oder Tools wie who.is kannst du herausfinden, wann eine Domain registriert wurde. Wenn die Seite erst seit 2 Wochen existiert: Finger weg!

8. Keine AGB oder Datenschutzerklärung

Oder sie sind da, aber in schlechtem Deutsch und ohne klare Informationen – oder sogar kopiert von anderen Seiten.

9. Fehlende Kundenbewertungen außerhalb des Shops

Gib den Shopnamen mal bei Google + „Erfahrungen" oder „Betrug" ein. Oft findest du bereits Warnungen von anderen Nutzern oder Verbraucherschutzseiten.

10. Du findest den Shop nur über Werbung

Viele Fake-Shops werden ausschließlich über Social Media Ads beworben – dort geben sie richtig Gas, um möglichst viele Leute in kurzer Zeit zu ködern. Danach verschwinden sie und tauchen unter neuer Adresse wieder auf.

Besonders oft betroffen:

- Mode & Markenklamotten
- Sneaker & Schuhe (z. B. Nike, Adidas, Converse)
- Elektronik & Smartphones
- Möbel und Gartenartikel
- Spielsachen & Lego-Fälschungen
- Werkzeuge & Heimwerkerbedarf

Was tun, wenn du hereingefallen bist?

- Bank kontaktieren / Zahlung stornieren
- Wenn du per Kreditkarte oder SEPA bezahlt hast, kann man oft rückbuchen lassen.
- Anzeige bei der Polizei erstatten
- Auch wenn die Täter schwer zu fassen sind – jede Anzeige hilft, Muster zu erkennen.
- Verbraucherschutz informieren
- Die Verbraucherzentralen sammeln Fake-Shops und warnen davor.
- Zukünftig vorsichtiger sein

Klingt banal, aber: Man lernt draus. Je öfter du die Warnzeichen erkennst, desto schwerer wirst du beim nächsten Mal reingelegt.

Fazit - Wachsamkeit ist der beste Schutz! Fake-Shops sind raffiniert gemacht, arbeiten mit psychologischen Tricks (Druck, Verknappung, Superrabatte) – und sie tauchen jeden Tag neu auf.

Aber wenn du dir die 10 Warnzeichen einprägst und lieber zwei Minuten länger prüfst, kannst du dich gut schützen.

Denn: Günstig ist nicht immer billig. Und manchmal ist billig verdammt teuer.

Empfehlenswerte Quellen

Wikipedia: Fake Shops
https://de.wikipedia.org/wiki/Fakeshop

Verbraucherzentrale: Fake-Shops erkennen und vermeiden
https://www.verbraucherzentrale.de/fakeshopfinder-71560

Bundesamt für Sicherheit in der Informationstechnik (BSI): Sicheres Einkaufen im Netz
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Online-Banking-Online-Shopping-und-mobil-bezahlen/Online-Shopping/online-shopping_node.html

Watchlist Internet: Fakeshops – Gefahren und Schutzmaßnahmen
https://www.watchlist-internet.at/fake-shops/

Whois-Abfrage: Domainprüfung
https://who.is/

YouTube: Schnäppchen finden, Betrug erkennen, sicher zahlen: Tipps zum Online-Shopping | c't uplink
https://www.youtube.com/watch?v=Mh9H-pS9dGg

Glänzende Sterne, faule Tricks

Wie Fake-Bewertungen entstehen und wie du sie erkennst

Du suchst einen neuen Toaster. Oder ein Hotel für den Sommerurlaub. Oder die besten Bluetooth-Kopfhörer unter 50 Euro. Und da ist er auch schon – der Geheimtipp, der alles kann, alles hat und von 273 Menschen mit 5 Sternen bewertet wurde. Klingt zu gut, um wahr zu sein?

Ist es oft auch.

Denn willkommen in der Welt der Fake-Bewertungen – dem Paralleluniversum des Internets, in dem mittelmäßige Produkte zu Bestseller-Sternchen werden, Hotels plötzlich sauber sind und Zahnaufheller über Nacht dein Leben verändern.

Was sind Fake-Bewertungen eigentlich?

Fake-Bewertungen sind gefälschte Kundenmeinungen, die auf Bewertungsplattformen, in Online-Shops oder bei Google Maps auftauchen – mit dem Ziel, ein Produkt oder Unternehmen besser (oder manchmal schlechter) darzustellen, als es wirklich ist.

Man unterscheidet dabei zwischen:

- Positiven Fake-Bewertungen (gekauftes Lob)
- Negativen Fake-Bewertungen (gekaufter Rufmord)
- Automatisierten Bewertungen (durch Bots generiert)
- Fake-Bewertungen durch “Freunde & Familie” (meist kostenlos, aber auch nicht objektiv)

Woher kommen Fake-Bewertungen?

1. Gekauft auf dem Schwarzmarkt

Ja, wirklich: Es gibt Plattformen, Foren und Telegram-Gruppen, in denen Anbieter gegen Bezahlung Bewertungen schreiben – oft gleich in Massen.

Beispiele:

- „50 Amazon-Bewertungen für 99 €“
- „Trustpilot-Boost – 5 Sterne für deinen Shop“
- „TripAdvisor-Ratings ab 1 € pro Stück“

Viele dieser Dienste stammen aus Ländern mit niedrigem Lohnniveau (z. B. Indien, Bangladesch, Pakistan) – dort schreiben Freelancer in Massen Bewertungen auf Deutsch, Englisch oder Französisch, obwohl sie das Produkt nie in der Hand hatten.

2. Bewertung gegen Produkt

Ein beliebter Trick: Man schickt das Produkt kostenlos an Menschen, die im Gegenzug eine positive Bewertung schreiben.

Meistens über Amazon oder andere Plattformen. Viele dieser Bewertungen beginnen mit: „Ich habe dieses Produkt vergünstigt erhalten, aber meine Meinung bleibt ehrlich.“ (Spoiler: Bleibt sie oft nicht.)

3. Eigene Mitarbeiter oder Agenturen

Manche Firmen lassen intern schreiben oder beauftragen externe Agenturen, die „Reputation Management“ betreiben – ein netter Begriff für „Imagepolitur durch gefälschte Bewertungen“.

Warum sind Fake-Bewertungen problematisch?

- Sie täuschen Verbraucher: Du kaufst etwas, das nicht hält, was die Sterne versprechen.
- Sie verzerren den Wettbewerb: Schlechte Produkte landen ganz oben, gute verschwinden.
- Sie erschüttern das Vertrauen: Wenn du einmal reingefallen bist, glaubst du auch echten Bewertungen irgendwann nicht mehr.

Wie erkennt man Fake-Bewertungen? – Die besten Tricks!

Hier eine kleine Detektivausrüstung für den digitalen Alltag:

1. Zu viele 5-Sterne-Bewertungen in kurzer Zeit

Wenn ein Produkt plötzlich innerhalb weniger Tage Dutzende Top-Bewertungen bekommt – und das bei einem unbekannten Anbieter – solltest du skeptisch werden.

2. Übertrieben positives Vokabular

Wenn jede Bewertung klingt wie eine Werbeanzeige, z. B.: „Ich bin absolut begeistert! Dieses Kabel hat mein Leben verändert! Nie wieder ohne!“ Das riecht stark nach Copy-Paste. Echte Menschen schreiben nicht so.

3. Kaum Kritik – oder nur belanglose Kritik

Wenn alle sagen:

„Perfekt! Nur die Verpackung war ein bisschen zerdrückt…“ „Super zufrieden! Lieferung dauerte einen Tag länger – aber egal.“ …dann wurden oft bewusst „weiche“ Schwächen eingebaut, um den Eindruck von Echtheit zu erwecken.

4. Rezensent hat nur dieses eine Produkt bewertet

Klick mal auf den Namen des Rezensenten. Wenn dort steht:

„1 Bewertung“ ...und das ist ausgerechnet dieses Produkt, ist das verdächtig. Noch verdächtiger: Ein Nutzer hat in einer Woche 25 Produkte bewertet – vom Hundehalsband bis zur Damenstrumpfhose.

5. Wiederholungen & gleiche Formulierungen

Viele Fake-Bewertungen sehen sich erschreckend ähnlich. Besonders bei günstig eingekauften Massen-Bewertungen wird oft ein Text mehrfach leicht abgeändert.

Beispiel:

- „Das Produkt kam schnell an und ist sehr hochwertig verarbeitet.“
- „Schnelle Lieferung, super Qualität, sehr hochwertig.“

Zufall? Kaum.

Hilfreiche Tools und Plattformen zur Erkennung

- Fakespot (fakespot.com)
  - Bewertet Amazon-, Yelp- und Tripadvisor-Seiten auf Vertrauenswürdigkeit.
- ReviewMeta (reviewmeta.com)
  - Erkennt manipulierte Amazon-Bewertungen und filtert sie heraus.
- Browser-Plugins wie „ReviewCheck“
  - Markieren auffällige Bewertungen direkt auf der Shopseite.

Welche Plattformen sind besonders betroffen?

- Amazon – Vor allem bei günstigen Elektronik-Gadgets und Noname-Marken
- Google Maps / Google My Business – Beliebt bei lokalen Dienstleistern
- TripAdvisor & HolidayCheck – Hotels, Ferienwohnungen, Restaurants
- Trustpilot – Viele Shops „kaufen" sich dort 5 Sterne
- App Stores – Auch App-Entwickler manipulieren Bewertungen, um in den Charts zu steigen

Wie kannst du dich schützen?

- Lies auch die 1- bis 3-Sterne-Bewertungen
- Filtere nach „neueste Bewertungen zuerst"
- Nutze Vergleichsportale, die unabhängig testen (z. B. Stiftung Warentest, Chip, heise)
- Verlasse dich nicht auf eine Plattform allein
- Wenn möglich: Bewertungen mit Fotos und echten Details bevorzugen

Fazit - Kritisch denken hilft – auch bei 5 Sternen

Nicht jede gute Bewertung ist gelogen. Aber: Nicht jede Bewertung ist echt. Je professioneller Fake-Bewertungen aussehen, desto schwerer sind sie zu erkennen – doch mit einem geübten Auge und ein paar Hilfsmitteln kannst du die Spreu vom Sternenglanz trennen.

Denn am Ende gilt wie so oft im Internet: „Wenn es zu gut klingt, um wahr zu sein – ist es meistens auch nicht wahr."

Empfehlenswerte Quellen

Wikipedia: Fake Review
https://en.wikipedia.org/wiki/Fake_review

Verbraucherzentrale: Fake-Bewertungen erkennen
https://www.verbraucherzentrale.de/wissen/digitale-welt/e-commerce/fakebewertungen-im-internet-erkennen-und-vermeiden-24414

Bundesverband der Verbraucherzentralen (vzbv): Fake-Bewertungen im Netz
https://www.vzbv.de/pressemitteilungen/fake-bewertungen-im-internet-eine-wachsende-gefahr

Heise Online: Amazon kämpft gegen Fake-Bewertungen
https://www.heise.de/news/Amazon-Angriff-auf-Fake-Bewertungen-6191912.html

Golem.de: ReviewMeta und Fakespot im Einsatz
https://www.golem.de/news/fake-bewertungen-reviewmeta-und-fakespot-2104-156315.html

Tools und Plattformen:

Fakespot (zur Überprüfung der Vertrauenswürdigkeit von Produktbewertungen)
https://www.fakespot.com/

ReviewMeta (zur Analyse und Filterung gefälschter Amazon-Bewertungen)
https://reviewmeta.com/

Likes, Lügen, Luxus

Wie Influencer & YouTuber mit deinem Klick Geld machen

Willkommen in der Welt der Filter, Rabattcodes und gesponserten Lebensstile!

Hier wird morgens ein „authentischer Morgenkaffee“ mit einem frisch zugeschickten Milchaufschäumer zelebriert, danach gibt’s ein Workout mit gesponserter Sportkleidung, und zum Abendbrot kommt die vegane Fertigpizza – natürlich mit Affiliate-Link – auf den Tisch. Klingt nach einem normalen Tag im Leben eines Influencers oder YouTubers.

Aber was steckt eigentlich hinter dieser perfekt inszenierten Online-Realität?

Wie verdienen diese Menschen ihr Geld – und warum promoten sie Produkte, die sie selbst oft nicht einmal benutzen würden?

Setz dich, schnapp dir deinen (selbst gekauften) Kaffee – wir schauen genauer hin.

Was ist eigentlich ein Influencer?

Laut Wikipedia bezeichnet ein Influencer (engl. „to influence“ = beeinflussen) eine Person, die in sozialen Medien eine große Reichweite und einen hohen Grad an Vertrauen bei ihrer Zielgruppe genießt – und genau dieses Vertrauen für Marketingzwecke nutzt.

Ein Influencer ist also so etwas wie der coole Typ aus der Schule, dem plötzlich alle dieselbe Jacke nachkaufen. Nur in digital, mit Ringlicht und bezahlter Kooperation.

YouTuber gehören übrigens zur Königsklasse der Influencer – weil sie nicht nur posten, sondern ganze Shows, Reviews und Vlogs inszenieren. Und das in einem Maß, das mancher Fernsehsender vor Neid erblassen lässt.

Wie verdienen Influencer & YouTuber ihr Geld?

Es gibt gleich mehrere Wege – viele davon sind verdammt lukrativ:

1. Werbung & Sponsoring
Eine Firma bezahlt direkt für die Erwähnung eines Produkts.

Beispiel: „Danke an XY-Kopfhörer, die mir diesen Vlog überhaupt erst ermöglicht haben!“

Die Sätze sind vorher meist abgestimmt – und das Produkt taucht zufällig mehrfach im Video oder Post auf.

2. Affiliate-Marketing
Ein Link mit einem Code wie „MARC10“ führt zu einem Shop. Wenn du etwas kaufst, bekommt der Influencer Prozente vom Umsatz – oft 5–15 %, bei digitalen Produkten manchmal mehr.

Du kaufst also Zahnpasta – und der Creator bekommt dafür ein Flugticket nach Ibiza.

3. Produktplatzierungen (Product Placement)
Die besonders elegante Form: Ein Produkt wird im Content eingebaut, ohne dass es wie klassische Werbung aussieht. Das Shampoo steht ganz zufällig im Hintergrund – aber rate mal, wovon es plötzlich überall Anzeigen gibt.

4. nEigene Produkte / Merch / Onlinekurse

Irgendwann wird der Influencer selbst zur Marke. Dann gibt's eigene T-Shirts, Nahrungsergänzungsmittel, E-Books oder – besonders beliebt – „Exklusive Online-Coachings".

„Lerne in meinem Kurs, wie auch du Influencer wirst und aus deinem Wohnzimmer ein Lamborghini-Parkhaus machst."

Das große Problem: Authentizität vs. Werbung

Viele Influencer verkaufen sich als „ganz normale Leute wie du und ich".

Sie erzählen persönliche Geschichten, zeigen sich im Jogginganzug mit Pickel im Gesicht – und das ist kein Zufall. Denn Nähe schafft Vertrauen.

Dieses Vertrauen wird dann genutzt, um dir Dinge zu empfehlen, die sie selbst nie kaufen würden, oft nicht mal auspacken. Der Lippenstift, die Gaming-Maus, die „revolutionäre" Abnehm-Kapsel: Alles landet nur im Video, weil dafür gezahlt wurde.

In vielen Fällen ist das irreführende Werbung, insbesondere wenn sie nicht korrekt gekennzeichnet wird (und das passiert leider immer noch oft). Die Trennung zwischen Werbung und Meinung verschwimmt – was im klassischen Journalismus undenkbar wäre.

Wie viel Geld ist da wirklich im Spiel?

Ein Influencer mit 100.000 Followern auf Instagram kann mehrere tausend Euro pro Post verlangen.

Auf YouTube sind die Einnahmen besonders vielfältig: Neben Werbung über den YouTube-Partnerprogramm (etwa 1–5 € pro 1.000 Aufrufe) kommen Sponsorings, Affiliate-Links und eigene Produkte dazu.

Top-Creator verdienen sechsstellige Summen pro Monat.

Das bedeutet: Wer seine Followerschaft clever monetarisiert, verdient mit einem simplen Video mehr als manche Leute im Jahr.

Und je jünger die Zielgruppe, desto leichter funktioniert das – leider.

Die Masche: „Kauf das, du wirst wie ich“

Die psychologische Formel ist simpel:

„Ich bin cool, ich nutze Produkt XY – also wirst du auch cool, wenn du es kaufst.“

Was früher durch Stars in Fernsehwerbung gemacht wurde, passiert heute subtiler, authentischer – und direkter auf dem Smartphone.

Der große Unterschied: Influencer inszenieren sich als Freunde, nicht als Verkäufer. Und das macht sie so effektiv.

Warum das problematisch ist?

- Junge Zielgruppen sind leicht zu beeinflussen
- Kinder und Teenager sehen ihre Lieblingsinfluencer als Vorbilder – und merken oft nicht, dass es sich um gezielte Verkaufsstrategien handelt.
- Fehlende Kennzeichnung
- Obwohl laut Gesetz Werbung klar gekennzeichnet werden muss, machen es viele Influencer bewusst vage – mit Phrasen wie „In freundlicher Zusammenarbeit“, die niemand richtig versteht.
- Unrealistische Erwartungen
- Die gezeigte Lebenswelt ist oft künstlich. Produkte werden übertrieben positiv dargestellt – Probleme, Nebenwirkungen oder echte Erfahrungen? Fehlanzeige.
- Konsumdruck & FOMO (Fear of Missing Out)
- Die ständige Präsentation neuer Produkte erzeugt bei Zuschauern das Gefühl, etwas zu verpassen – und das kurbelt wiederum den Konsum an.

Fazit - Unterhaltung, ja – blinder Konsum, lieber nicht

Influencer & YouTuber können kreativ, unterhaltsam und inspirierend sein.

Viele leisten gute Arbeit, produzieren hochwertigen Content und sind transparent in ihrer Werbung.

Aber: Das Geschäftsmodell basiert oft darauf, dass Menschen Dinge kaufen, die sie nicht brauchen, nur weil jemand mit Ringlicht sie empfohlen hat.

Ein bisschen Vorsicht – und kritisches Hinterfragen – hilft dabei, nicht zum Dauer-Käufer auf Abruf zu werden.

Also das nächste Mal, wenn du denkst: „Boah, der Smoothiemixer sieht richtig geil aus… und MARIE20 gibt auch noch 20 % Rabatt!“ … atme tief durch, schließ kurz die App – und frag dich: „Würde ich das Ding auch kaufen, wenn es nicht gerade von einer Person mit Perfect-Skin-Filter in die Kamera gehalten wird?“

Wenn du dann immer noch willst – go for it.

Aber denk daran: Dein Klick ist bares Geld wert.
Vielleicht mehr, als du denkst.

Empfehlenswerte Quellen

Wikipedia: Influencer
https://de.wikipedia.org/wiki/Influencer

Wikipedia: Affiliate-Marketing
https://de.wikipedia.org/wiki/Affiliate-Marketing

Bundesverband Digitale Wirtschaft (BVDW): Influencer-Marketing Leitfaden
https://www.bvdw.org/publikationen/influencer-marketing-leitfaden/

Heise Online: Warum Influencer Werbung besser verkaufen als klassische Werbung
https://www.heise.de/news/Influencer-Werbung-mit-Vertrauensbonus-6005007.html

Golem.de: Werbeeinnahmen bei YouTube und Instagram
https://www.golem.de/news/youtube-und-instagram-wie-viel-influencer-verdienen-2112-162128.html

Markenverband / Influencer-Studie
https://www.markenverband.de/themen/influencer-marketing/

YouTube: Kann jeder Influencer werden? - So verdienen Influencer ihr Geld.
https://www.youtube.com/watch?v=KUjCKSRN-Q0

Warum du nie deine Haupt-E-Mail-Adresse benutzen solltest

und wie du dich clever vor Spam schützt

Deine E-Mail-Adresse ist wie deine Telefonnummer: Gibst du sie an die falschen Leute, klingelt's irgendwann ständig – und meistens ist es jemand, der dir was verkaufen will.

Viele Menschen machen den gleichen Fehler: Sie nutzen eine einzige E-Mail-Adresse für alles – Online-Shops, Newsletter, Social Media, Steuer, Arzttermine, Streaming, Fitnessstudio, ... und wundern sich dann über eine überquellende Inbox und gefährlichen Datenmüll.

Die gute Nachricht: Es gibt eine einfache Lösung – und sie liegt oft direkt vor deiner Nase.

Die Hauptadresse ist dein Login-Schlüssel, nicht deine Allzweckwaffe

Wenn du dich bei einem E-Mail-Anbieter wie Gmail, Outlook, ProtonMail, Tutanota, GMX oder Yahoo anmeldest, bekommst du automatisch eine Hauptadresse. Diese ist nicht nur deine erste E-Mail-Adresse, sondern gleichzeitig auch dein Login-Name für den Zugang zu deinem Postfach.

Aber – und das ist entscheidend:
Diese Login-Adresse solltest du niemals im Alltag verwenden.

Warum?

Sie ist dein digitaler Haustürschlüssel. Wenn sie geleakt wird, bist du ein leichtes Ziel für Phishing oder Spam. Sie lässt sich nicht so leicht ändern wie zusätzliche Adressen.

Fast jeder Anbieter erlaubt dir, weitere E-Mail-Adressen zu erstellen – und das solltest du nutzen

Viele Menschen wissen es gar nicht, aber: Nahezu jeder größere E-Mail-Anbieter erlaubt es, mehrere Adressen unter einem Account zu verwalten. Diese zusätzlichen Adressen heißen:

- Aliase (z. B. bei Microsoft Outlook, Gmail, Tutanota, iCloud)
- Zusätzliche Postfächer oder Subadressen
- Adressen mit Plus-Zusatz (z. B. deinname+shop @gmail.com)

Diese Adressen sind perfekt, um dein digitales Leben aufzuräumen.

Du kannst sie z. B. so aufteilen:

- vorname+privat@anbieter.de für Freunde & Familie
- vorname+shop@anbieter.de für Online-Bestellungen
- vorname+news@anbieter.de für Newsletter
- vorname+spam@anbieter.de für dubiose Gewinnspiele
- vorname+urlaub@anbieter.de für Reiseportale

Alle Mails landen trotzdem in deinem Hauptpostfach – du kannst sie aber nach Adressen filtern oder automatisch in Ordner sortieren lassen.

Und das Beste: Wenn eine Adresse zu viel Spam bekommt, schaltest du sie einfach ab oder ignorierst sie. Dein Haupt-Login bleibt dabei unberührt.

Vorteile dieser Methode

- Mehr Kontrolle: Du erkennst sofort, wer deine Adresse weitergegeben hat.
- Weniger Risiko: Bei Datenlecks ist nicht gleich dein ganzer Account betroffen.
- Mehr Übersicht: Automatische Filter sortieren Mails nach Zweck oder Quelle.
- Leichtere Pflege: Du kannst gezielt eine „Spam-Adresse" löschen, ohne alles zu verlieren.

Ein praktisches Beispiel

Stell dir vor, du meldest dich bei einem Online-Shop an, der drei Monate später gehackt wird. Deine Adresse landet in einem Datenleck – und plötzlich bekommst du Spam.

Wenn du nun deine Hauptadresse max.mustermann@gmail.com verwendet hast, hast du ein Problem. Aber wenn du max+shop@gmail.com verwendet hast, weißt du sofort, woher der Spam kommt – und kannst diese Adresse einfach blockieren.

Fazit - Mehr Adressen, mehr Ruhe im Postfach! Deine E-Mail-Adresse ist kein Allzweckwerkzeug, sondern ein digitales Identitätsstück. Nutze sie bewusst. Trenne Wichtiges von Werbemüll. Und nutze die Funktionen deines Mail-Anbieters clever aus – sie sind oft kostenlos und unglaublich effektiv.

Denn am Ende gilt: Ein gutes E-Mail-Setup ist wie ein guter Spamfilter – man merkt erst, wie wichtig es ist, wenn's zu spät ist.

Empfehlenswerte Links:

Wikipedia: E-Mail-Adresse
https://de.wikipedia.org/wiki/E-Mail-Adresse

Wikipedia: Alias-Adresse
https://de.wikipedia.org/wiki/Alias-Adresse

Gmail Hilfe: E-Mail-Aliase und Plus-Adressen verwenden
https://support.google.com/mail/answer/12096?hl=de

Microsoft Support: Erstellen eines Alias für Outlook.com
https://support.microsoft.com/de-de/office/hinzufügen-oder-entfernen-eines-e-mail-alias-in-outlook-com-459b1989-356d-40fa-a689-8f285b13f1f2

ProtonMail Support: Nutzung von Aliases und Plus-Tagging
https://proton.me/support/addresses-and-aliases

Tutanota FAQ: E-Mail-Alias erstellen
https://tuta.com/de/blog/secure-email-alias

Achtung Spam!

Wie du betrügerische E-Mails erkennst und dich richtig schützt

In einer idealen digitalen Welt würde unser Posteingang nur Mails von Menschen enthalten, die wir mögen – oder von Diensten, die wir tatsächlich nutzen. Aber stattdessen quillt er oft über mit dubiosen Nachrichten:

“Ihr Konto wurde gesperrt!” – “Jetzt 500 € Amazon-Gutschein sichern!” – “Wichtige Nachricht zu Ihrer Sendung” – oder einfach nur ein Anhang mit dem unschuldig wirkenden Titel “Rechnung.pdf”.

Herzlichen Glückwunsch, du hast Spam!
Und je nach Absender ist das harmlos oder brandgefährlich.

Deshalb gilt: Wissen ist der beste Spamfilter.

Was ist Spam überhaupt?

Ursprünglich bezeichnete man mit „Spam“ nur unerwünschte Werbung per E-Mail – inzwischen ist es ein Sammelbegriff für alles, was in deinem Posteingang nichts verloren hat. Dazu gehören:

- Werbung für zweifelhafte Produkte oder Dienstleistungen
- Phishing-Mails, die Passwörter oder Zahlungsdaten abgreifen wollen
- Mails mit Schadsoftware im Anhang
- Betrügerische Gewinnversprechen oder Jobangebote
- Falsche Rechnungen oder Mahnungen

Nicht jede Spam-Mail ist gefährlich – aber viele sind es.

So erkennst du Spam-Mails – 8 Warnzeichen, auf die du achten solltest

1. Ungewöhnlicher Absender

Du bekommst eine Mail von “Sparkasse Kundenservice”, aber die Absenderadresse lautet service@kundenzentrum-rg87.info. Achte immer auf die vollständige Adresse! Große Firmen nutzen nie kryptische Domains.

2. Druck, Drohung oder Panikmache

Typische Formulierungen sind:

- “Ihr Konto wird in 24 Stunden gesperrt!”
- “Letzte Mahnung!”
- “Sie wurden gehackt – ändern Sie sofort Ihr Passwort!”

Seriöse Anbieter kommunizieren nie auf diese Weise.
Panik ist ein Werkzeug von Betrügern.

3. Rechtschreib- und Grammatikfehler

Viele Spam-Mails werden automatisch aus fremden Sprachen übersetzt – und das merkt man: “Ihre konto nicht sicher. Bitte klicken.”

Komische Satzstellung? Falsche Umlaute? Hände weg!

4. Verlockende Versprechen

- “Sie haben gewonnen!”
- “Nur heute: iPhone für 1 €!”
- “Staat zahlt dir 3000 € Bonus!”

Wenn es zu gut klingt, um wahr zu sein, ist es meistens auch nicht wahr.

5. Seltsame Links

Spam-Mails enthalten fast immer Links, die dich zu gefälschten Seiten führen. Tipp: Fahr mit der Maus über den Link (nicht klicken!) – dann siehst du unten im Browser, wohin er wirklich führt.

6. Ungewöhnliche oder leere Anhänge

ZIP-Dateien, Word-Dokumente oder PDFs mit neutralen Namen wie „Rechnung“ oder „Mahnung“ enthalten oft Trojaner oder Viren. Öffne niemals Anhänge, die du nicht erwartest.

7. Allgemeine Anrede

„Sehr geehrter Kunde“ oder „Hallo Nutzer“ – statt deines echten Namens? Ein klares Zeichen für Massenversand.

8. Unerwartete E-Mails

Wenn du keine Bestellung aufgegeben hast, bekommst du auch keine Sendungsverfolgung. Vertraue deinem Bauchgefühl: Kommt dir die Mail komisch vor, ist sie es vermutlich auch.

Wie du richtig auf Spam reagierst – und was du auf keinen Fall tun solltest

1. Nicht antworten

Auch keine nette Bitte wie: „Bitte löschen Sie mich aus dem Verteiler“ – das zeigt nur, dass deine Adresse aktiv ist.

2. Nicht klicken

Kein Link, kein Button, kein “Hier überprüfen” – einfach ignorieren. Ein Klick kann schon eine Weiterleitung oder eine Malware-Ausführung auslösen.

3. Nicht öffnen (wenn offensichtlich gefährlich)

Einige Mailprogramme zeigen automatisch Bilder an – was Spammern verrät, dass du die Mail gesehen hast. Deshalb: Bilder nicht automatisch laden lassen.

4. Als Spam markieren

Nutze den „Spam melden“-Button deines Mailprogramms. Dadurch lernt dein Mailanbieter, ähnliche Mails in Zukunft direkt auszusortieren – das hilft dir und der ganzen Community.

5. Löschen

Der beste Freund jeder Inbox.

Zusätzlicher Schutz: Spamfilter & clevere Adressen nutzen

Gute E-Mail-Anbieter wie Gmail, Outlook, Tutanota oder ProtonMail haben bereits intelligente Spamfilter integriert. Du kannst aber selbst noch nachhelfen: Filterregeln erstellen, z. B. „Wenn Betreff ‘Mahnung’ und Absender nicht bekannt → Papierkorb“

Achtung: Phishing ist besonders gefährlich

Phishing-Mails sehen täuschend echt aus – sie kommen scheinbar von deiner Bank, Amazon oder PayPal. Sie führen auf gefälschte Webseiten, die das Original perfekt kopieren.

Nie über einen Link in der Mail einloggen! Gib stattdessen selbst die offizielle Adresse im Browser ein und logge dich dort ein.

Fazit - Digitales Misstrauen ist kein Zeichen von Paranoia – sondern von gesundem Menschenverstand

Spam-Mails sind die Kakerlaken des Internets: schwer zu beseitigen, hartnäckig und manchmal gefährlich. Mit dem richtigen Wissen kannst du ihnen aber gelassen begegnen.

Im Zweifel gilt: Erst denken, dann klicken. Und manchmal lieber einfach löschen.

Empfehlenswerte Quellen

Wikipedia: Spam (E-Mail)
https://de.wikipedia.org/wiki/Spam_(E-Mail)

Bundesamt für Sicherheit in der Informationstechnik (BSI):
So können Sie sich vor Spam schützen
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Spam/Wie-schuetzt-man-sich-vor-Spam/wie-schuetzt-man-sich-vor-spam_node.html

Heise Online: Phishing erkennen und vermeiden
https://www.heise.de/tipps-tricks/Phishing-erkennen-und-vermeiden-4991403.html

Wie man E-Mail-Phishing-Angriffe verhindert - eine Anleitung.
https://tutanota.com/de/blog/posts/phishing/

ProtonMail Blog: 11 Tipps, um Spam-E-Mails zu stoppen
https://proton.me/blog/de/how-to-stop-spam-emails

YouTube: Was ist Spam? Unerwünschte elektronische Nachrichten und wie ihr euch davor schützen könnt!
https://www.youtube.com/watch?v=x-pElhZ9xH8

Unsichtbare Spione im Posteingang

Wie uns E-Mails mit Bildern heimlich tracken – und warum du deinem Postfach nicht trauen solltest

Die E-Mail: harmlos oder horchend?

„Sie haben eine neue Nachricht!" – klingt harmlos, oder? Vielleicht ist es ein Newsletter, vielleicht ein Gutschein oder ein Gruß von Tante Helga. Was die meisten aber nicht wissen: Mit dem Öffnen der E-Mail öffnet man auch oft eine Tür in die eigene digitale Privatsphäre. Und der Übeltäter? Ein Bild.

Aber kein hübsches Urlaubsfoto oder animiertes Katzen-GIF. Nein – es ist meist ein unsichtbares, 1x1 Pixel kleines Bild namens Tracking-Pixel, das aussieht wie… gar nichts. Und genau das ist das Problem.

Wie funktioniert E-Mail-Tracking mit Bildern?

Das Prinzip ist so einfach wie perfide:

- In die E-Mail wird ein Bild eingebettet, das nicht direkt in der Mail steckt, sondern von einem externen Server nachgeladen wird
- Sobald du die E-Mail öffnest, lädt dein Mailprogramm dieses Bild – und der Server merkt: Aha, geöffnet!
- Dabei kann der Absender feststellen:
- Wann du die E-Mail geöffnet hast
- Wie oft du sie geöffnet hast
- Wo du dich ungefähr aufhältst (über deine IP-Adresse)
- Welches Gerät und welchen Mailclient du benutzt
- Und ob du der Typ bist, der nachts um 2 Uhr Spam liest

Manche Tracker gehen sogar so weit, dir in der URL eine ID zu geben, um dein Verhalten über verschiedene E-Mails hinweg zu analysieren. Willkommen im digitalen Zoo!

Wer macht sowas?

- Newsletter-Versender: Von legitimen Anbietern wie Online-Shops bis hin zu windigen Influencern mit „einem großartigen Coaching-Angebot!“
- Marketingfirmen: Für sie ist jede Öffnung ein wertvoller Datenpunkt.
- Phishing-Angreifer: Die wissen dadurch, ob deine E-Mail-Adresse „lebt“ – und schicken dir dann noch viel kreativere Abzockversuche.
- Politische Organisationen: Wer wissen will, ob seine Kampagne zieht, trackt die Klicks, Öffnungen und Reaktionen… und vielleicht auch gleich deine Meinung.

Und was hat das mit „Überbelastung“ zu tun?

Je mehr solche Tracker in den E-Mails stecken, desto mehr:

- …wird dein Postfach zur Daten-Melkmaschine,
- …wird dein Gerät mit ungewollten Anfragen bombardiert,
- …wirst du zum gläsernen Leser ohne Lesebrille.

Dazu kommt: Manche E-Mail-Programme laden auch gleich externe Skripte oder Stylesheets mit nach – besonders in Webmail-Clients. Das ist so, als würde man einem Paketboten erlauben, auch gleich mal das Wohnzimmer zu scannen, bevor er das Päckchen ablegt.

Was kann man dagegen tun?

Die gute Nachricht: Es gibt Schutzmaßnahmen. Die schlechte: Viele sind standardmäßig nicht aktiv.

Automatisches Laden von Bildern deaktivieren!

Fast jedes Mailprogramm erlaubt es, externe Inhalte nur auf Anfrage zu laden. Beispiel:

- Gmail: „Bilder von unbekannten Absendern nicht automatisch anzeigen."
- Outlook: „Automatisches Herunterladen von Bildern verhindern."
- Apple Mail: Bilder blockieren (in aktuellen iOS-Versionen sogar mit Anti-Tracking-Schutz).

Privacy-fokussierte Mailclients verwenden!

ProtonMail, Tutanota oder Mailfence zeigen Bilder nicht automatisch an und blockieren Tracking-Elemente.

Browser-Plugins nutzen

Tools wie uBlock Origin oder Privacy Badger helfen auch bei Webmail-Diensten, Tracking-URLs zu blockieren.

E-Mail-Alias-Dienste

Wer nicht mit seiner echten Adresse unterwegs sein will, kann Dienste wie SimpleLogin oder Firefox Relay nutzen – so bleibt wenigstens das Profil etwas diffuser.

Fazit - Sag dem Pixel den Kampf an!

Die E-Mail wird überwacht, analysiert und mit Pixeln gespickt. Wer glaubt, mit einem harmlosen Öffnen nichts preiszugeben, hat noch nie die dunkle Seite des Posteingangs erlebt.

Aber mit ein paar Klicks und etwas Paranoia bist du auf der sicheren Seite. Oder wie die Ältesten des Internets sagen: „Trust no pixel."

Empfehlenswerte Quellen

Wikipedia
https://en.wikipedia.org/wiki/Web_beacon

YouTube: Tracking Pixels in Emails (They’re Spying on You)
https://www.youtube.com/watch?v=TC09ml9Fpg8

„Hallo, hier ist Microsoft“

Wie Betrüger per Telefon dein Geld und deinen PC kapern

Es beginnt oft harmlos: Das Telefon klingelt. Am anderen Ende spricht jemand mit indischem oder englischem Akzent, stellt sich freundlich als „Support-Mitarbeiter von Microsoft“ oder „Windows-Sicherheitszentrale“ vor – und behauptet, dein Computer habe ein schwerwiegendes Sicherheitsproblem.

Was danach passiert, ist ein digitales Drama in mehreren Akten – mit dir als Hauptopfer. Willkommen in der Welt der Tech-Support-Scams, einer besonders perfiden Form von Telefonbetrug.

Was sind Tech-Support-Scams?

Bei sogenannten Tech-Support-Scams geben sich Betrüger als Mitarbeiter von bekannten Firmen wie Microsoft, Amazon, Google, PayPal, Deutsche Telekom oder sogar deiner Hausbank aus. Ziel ist es, dein Vertrauen zu gewinnen – um anschließend:

- Zugriff auf deinen Rechner zu bekommen
- deine persönlichen Daten zu klauen
- dir angebliche Kosten aufzuschwatzen
- oder dich sogar zu erpressen

Diese Anrufe kommen nicht wirklich von Microsoft oder anderen Unternehmen – auch wenn der Anrufername oder die Telefonnummer gefälscht ist und seriös aussieht. Solche Betrugsversuche sind

international organisiert und oft Teil von kriminellen Callcenter-Netzwerken, z. B. aus Indien, Osteuropa oder Nordafrika.

So läuft ein typischer Fake-Anruf ab

1. Der Anruf kommt aus dem Nichts.

Meist ruft eine ausländische Nummer an – manchmal aber auch mit deutscher Vorwahl. Der Anrufer spricht gebrochen Deutsch oder Englisch.

2. Die Masche: „Ihr PC ist infiziert!“

Er behauptet, dein Rechner habe Viren, sei von Hackern übernommen worden oder verschicke Spam-Mails.

3. Er bietet Hilfe an – aber dafür brauchst du:

eine Fernwartungssoftware wie TeamViewer, AnyDesk oder Zoho Assist und musst dem „Mitarbeiter“ Zugriff auf deinen Rechner geben.

4. Du gibst ihm Kontrolle – und damit die Tür zu allem.

Jetzt sieht er deinen Bildschirm, kann Programme starten, Dateien kopieren oder löschen.

5. Und dann kommt der Trick mit der Bank: „Wir haben Ihnen Geld überwiesen…“

Der Betrüger behauptet plötzlich, dass dir fälschlicherweise zu viel Geld überwiesen wurde – oft mehrere Tausend Euro. Dabei zeigt er dir gefälschte Kontoauszüge oder manipuliert live die Webseite deiner Bank, während du drauf schaust.

Wie das geht?

Mit Browser-Manipulation, sogenannten Overlays oder kleinen Scripten, die während der Fernwartung installiert wurden. So siehst du ein „Plus“ auf deinem Konto – das in Wahrheit nie existiert hat.

Dann kommt die Erpressung:

- „Bitte überweisen Sie das Geld sofort zurück – sonst verlieren wir unseren Job.“
- Oder: „Wir müssen Ihre Karte sperren, wenn Sie nicht reagieren!“

Und plötzlich ist das Konto leer!

Viele Opfer, oft ältere Menschen oder technisch wenig versierte Nutzer, glauben die Geschichte, schicken wirklich Geld – z. B. über:

- Banküberweisung
- Kryptowährungen (Bitcoin etc.)
- Geschenkkarten (Apple, Google, Amazon)

Oder sie verlieren nicht nur ihr Geld, sondern auch ihre Zugangsdaten, Passwörter, private Dateien oder Fotos – und das Vertrauen in die digitale Welt gleich mit.

Wie erkenne ich einen Fake-Anruf?

- Microsoft ruft dich niemals ungefragt an.
- Ebenso wenig Amazon, Google oder deine Bank.
- Drohungen, Dringlichkeit oder Panikmache (“Ihr Computer wird in 10 Minuten gesperrt!”) sind typische Alarmzeichen.
- Ungewöhnliche Zahlmethoden wie Geschenkkarten, PayPal, oder Bitcoin sind eindeutige Hinweise auf Betrug.
- Schlechte Sprachqualität, Hintergrundgeräusche (Callcenter), gebrochenes Deutsch oder Englisch.

Was sollte man tun, wenn man so einen Anruf bekommt?

- Auflegen. Sofort. Ohne Diskussion.
- Keine Daten preisgeben. Niemals Fernzugriff gewähren.
- Nummer blockieren (auf dem Handy) oder bei der Bundesnetzagentur melden.

Wenn du Daten eingegeben hast:

- Bank oder Kreditkarte sofort informieren
- Computer vom Profi prüfen lassen
- Passwörter ändern
- Anzeige erstatten: bei der Polizei oder über die Onlinewache deines Bundeslandes.

Schutz-Tipp: Keine Fernwartungs-Tools installieren, die du nicht kennst

Programme wie TeamViewer, AnyDesk oder UltraVNC sind nützlich – aber in den falschen Händen brandgefährlich.

Installiere so etwas nur, wenn du genau weißt, mit wem du es zu tun hast – z. B. bei einer geplanten Support-Sitzung mit einem echten IT-Dienstleister.

Fazit - Vertrauen ist gut – Misstrauen ist besser

Die Anrufer klingen höflich, hilfsbereit und manchmal sogar kompetent. Aber kein echter Microsoft-Mitarbeiter ruft dich an, um dir einen Virus zu entfernen.

Und kein seriöser Support braucht Zugriff auf dein Konto, um dir „Geld zurückzugeben".

Diese Betrüger sind wahre Meister der Manipulation – und kombinieren psychologischen Druck mit technischem Know-how.

Empfehlenswerte Quellen

Wikipedia: Tech Support Scam
https://en.wikipedia.org/wiki/Technical_support_scam

Bundesamt für Sicherheit in der Informationstechnik (BSI):
Betrug durch gefälschte Telefonnummern und E-Mail-Adressen
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Gefaelschte-Absenderadressen/gefaelschte-absenderadressen_node.html

YouTube: Scammer "Erica Smith" bricht in Tränen aus !
https://www.youtube.com/watch?v=KvrhNhNQcp0

YouTube: HACKERS Reveal Criminal SECRETS On CCTV
https://www.youtube.com/watch?v=R0G9Sd7Fov4

YouTube: Wenn man Fake Microsoft Support Scammer anruft…
https://www.youtube.com/watch?v=Je0rje0XV4c

Was ist eigentlich die „Cloud“

und warum sollte man sich gut überlegen, wem man seine Daten anvertraut?

Stell dir vor, du hast eine riesige, unsichtbare Festplatte im Himmel, auf der du deine Urlaubsfotos, Steuerunterlagen, Liebesbriefe, Projekte und vielleicht sogar ein paar peinliche Selfies speicherst. Diese „unsichtbare Festplatte“ ist das, was wir Cloud nennen – auf Deutsch: Wolke. Klingt romantisch, ist aber hoch technisiert.

Die Cloud ist im Prinzip einfach ein externes Rechenzentrum, also ein Server (oder sehr viele davon), irgendwo auf der Welt. Statt deine Daten auf deinem eigenen Gerät zu speichern, schickst du sie ins Internet – und sie landen dort, wo der Cloud-Anbieter seine Server stehen hat.

Bekannte Anbieter sind z. B.:

- Google Drive (Alphabet/Google, USA)
- iCloud (Apple, USA)
- Dropbox (USA)
- OneDrive (Microsoft, USA)
- Nextcloud (Open Source, häufig in Deutschland gehostet)
- pCloud (Schweiz)
- Tresorit (Schweiz/Ungarn)

Warum das praktisch ist – aber auch heikel

Clouds sind unglaublich praktisch:

- Du kannst von überall auf deine Daten zugreifen.
- Du verlierst nichts, wenn dein Laptop stirbt.
- Du kannst Dateien mit anderen teilen.
- Dein Smartphone sichert automatisch Fotos in die Cloud.

Aber: Du gibst deine Daten damit aus der Hand.

Du verlagerst die Verantwortung von „deinem Gerät“ auf „jemand anders’ Server“ – und genau da wird es interessant, besonders beim Thema Datenschutz.

Datenschutz und staatlicher Zugriff – vor allem in den USA ein Problem

Wenn du einen Cloud-Dienst nutzt, musst du dem Anbieter vertrauen, dass er:

- deine Daten nicht analysiert (z. B. für Werbung),
- sie nicht weiterverkauft,
- sie gut vor Hackerangriffen schützt,
- sie nicht auf Anforderung einfach an Behörden herausgibt.

Gerade der letzte Punkt ist kritisch – besonders bei US-Anbietern.

Denn: In den USA gelten Gesetze wie der Patriot Act, der Cloud Act oder FISA (Foreign Intelligence Surveillance Act). Diese erlauben es

amerikanischen Behörden wie der NSA oder dem FBI, auf Daten zuzugreifen – auch dann, wenn die Server nicht in den USA stehen, solange die Firma amerikanisch ist.

Das heißt: Selbst wenn deine Daten auf einem Google-Server in Irland liegen – kann ein US-Gericht den Zugriff anordnen.

Und das muss nicht mal transparent passieren – viele dieser Datenanfragen sind mit Schweigepflicht verbunden.

Wie erkenne ich einen guten Cloud-Anbieter?

- Ein wirklich guter Cloud-Anbieter achtet auf:
- Ende-zu-Ende-Verschlüsselung

Deine Daten werden bereits auf deinem Gerät verschlüsselt, bevor sie in die Cloud gelangen – und nur du hast den Schlüssel. Selbst der Anbieter kann nichts lesen. Anbieter mit echter Ende-zu-Ende-Verschlüsselung sind z. B.:

- Tresorit
- Proton Drive
- pCloud (mit kostenpflichtiger Crypto-Option)
- Sync.co

Standort des Rechenzentrums / Firmensitz

Datenschutzfreundlich sind vor allem Länder wie:

- Deutschland
- Schweiz
- Island
- Norwegen

Meide möglichst Anbieter aus:

- USA (wegen CLOUD Act etc.)
- China (starke staatliche Kontrolle)
- Russland, Indien, VAE (eingeschränkte Datenschutzgesetze)

Open Source und Transparenz

Anbieter, die ihre Software offenlegen (wie Nextcloud), bieten mehr Kontrolle und Sicherheit, weil jeder den Quellcode prüfen kann.

Transparenzberichte zeigen, wie oft Behörden Daten angefragt haben.

Zertifizierungen und Datenschutzrichtlinien

Achte auf DSGVO-Konformität, ISO-Zertifikate und klar formulierte Datenschutzrichtlinien.

Gute Anbieter zeigen dir, wo genau deine Daten gespeichert werden – und was mit ihnen passiert.

Warum du deine Daten nicht „einfach irgendwo“ speichern solltest

Manche Leute sagen:

„Ich habe nichts zu verbergen – dann ist es doch egal, wo meine Daten liegen.“

Aber das ist so, als würdest du sagen:

„Ich habe nichts zu verbergen, also lasse ich meine Haustür offen.“ Auch wenn du nichts Illegales tust: Deine Daten sind persönlich. Sie gehören dir. Und wer darauf Zugriff hat, kann dein Verhalten analysieren, Profile erstellen, Werbung schalten, Meinungen beeinflussen – oder im schlimmsten Fall erpressen.

Fazit - Nicht jede Wolke ist eine gute Wolke

Cloud-Dienste sind heute ein fester Bestandteil unseres digitalen Lebens – und das ist auch okay.

Aber man sollte nicht blind alles hochladen, ohne sich zu fragen:

- Wo liegen meine Daten?
- Wer könnte sie lesen?
- Wie gut sind sie geschützt?

Wenn du es richtig machst, kann die Cloud ein sicherer, bequemer Speicherort sein.

Aber wie bei einem Schließfach: Du willst wissen, wer den Schlüssel hat – und ob der Anbieter nicht ab und zu selbst mal reinschaut.

Empfehlenswerte Quellen

Wikipedia: Cloud Computing
https://de.wikipedia.org/wiki/Cloud_Computing

Wikipedia: USA PATRIOT Act
https://de.wikipedia.org/wiki/USA_PATRIOT_Act

Wikipedia: CLOUD Act (Clarifying Lawful Overseas Use of Data Act)
https://en.wikipedia.org/wiki/CLOUD_Act

Nextcloud – Offizielle Webseite
https://nextcloud.com/

Tresorit – Offizielle Webseite
https://tresorit.com/

Proton Drive – Offizielle Webseite
https://proton.me/drive

Bundesamt für Sicherheit in der Informationstechnik (BSI): Cloud Computing Leitfaden
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sichere_Nutzung_Cloud_Dienste.pdf?__blob=publicationFile&v=1

YouTube: Was ist „die Cloud“? | ‘Frag doch Google’
https://www.youtube.com/watch?v=4F9PdEg3tNA

In der Endlosschleife

Warum uns YouTube Shorts & Co. so sehr fesseln – und was das mit unserer Realität macht

Kennst du das? Du wolltest nur kurz auf YouTube gehen, um dir ein Kochrezept anzusehen – und zwei Stunden später hast du keine Lasagne, aber einen Kopf voller „Lifehacks", Fail-Videos und einem Typen, der in 30 Sekunden 15 Eier isst.

Herzlichen Glückwunsch, du bist in die Kurzvideo-Falle geraten. Willkommen bei YouTube Shorts, Facebook Reels, TikTok & Co. – dem digitalen Kaugummi für dein Gehirn.

Doch warum funktioniert das so gut – und warum ist das manchmal ein echtes Problem?

Das Rezept für digitale Abhängigkeit: Warum Shorts so süchtig machen

1. Reizüberflutung in Mini-Portionen
Kurze Videos sind wie Chips:
Klein, salzig, intensiv – und du kannst einfach nicht aufhören.
Jedes Video bietet einen schnellen Dopamin-Kick:

- Lacher
- Emotionen
- Überraschungen
- „Aha"-Momente
- visuelle Reize im Sekundentakt

Das macht unser Gehirn wach, neugierig – und hungrig auf mehr.

Denn:
Je kürzer das Video, desto schneller kommt der nächste Kick.

2. Endloses Scrollen ohne Pause

- Die Apps haben keine „natürlichen Stopppunkte".
- Bei klassischen Videos oder Filmen ist irgendwann Schluss – bei Shorts kannst du theoretisch ewig weiterwischen.
- Es gibt keinen Abspann, keinen „The End"-Moment.
- Dein Daumen wird zum Hebel in einem Belohnungsspiel: Vielleicht ist das nächste Video noch besser!

Psychologisch gesehen ist das ein Mechanismus aus der Glücksspielwelt: Variable Belohnung – wie beim Spielautomaten.

3. Perfektes Targeting dank Algorithmen

Sobald du einem Video ein bisschen Aufmerksamkeit schenkst, merkt sich der Algorithmus:

- Worauf hast du länger geschaut?
- Worauf hast du reagiert?
- Was hast du übersprungen?

Er lernt dich besser kennen als dein bester Freund – und serviert dir mit chirurgischer Präzision mehr vom Gleichen.

Wenn du z. B. auf ein Video über Gaming klickst, folgen sofort 20 weitere Gaming-Videos – garniert mit Kommentaren wie „Diese Szene wird dich umhauen!“.

So landest du unmerklich in deiner ganz persönlichen Themen-Bubble.

Was ist eine Bubble – und warum ist sie gefährlich?

Eine Bubble (also Blase) entsteht, wenn du immer wieder ähnliche Inhalte zu sehen bekommst – und andere Themen, Perspektiven und Meinungen ausgeblendet werden.

Das wirkt harmlos, ist aber in Wahrheit ein schleichender Prozess:

- Du verlierst den Überblick über die Vielfalt der Welt.
- Du denkst, „alle“ interessieren sich für das, was du auch magst.
- Deine eigene Meinung wird verstärkt, aber nie herausgefordert.
- Du bekommst das Gefühl: „Ich liege immer richtig – und alle anderen sind komisch.“

Das kann dazu führen, dass man sich von der Realität entfernt – besonders bei politischen, gesellschaftlichen oder weltanschaulichen Themen.

Was macht das mit uns – psychisch und sozial?

Konzentrationsprobleme: Durch den ständigen Input fällt es schwerer, sich auf längere Inhalte zu konzentrieren – ein Buch zu lesen,

einen Film ohne Handy zu schauen oder einfach mal zehn Minuten still zu sitzen.

Vergleichsdenken & Unzufriedenheit: Du siehst ständig Menschen, die schöner, reicher, cooler oder erfolgreicher wirken als du. Was du nicht siehst: Die echten Geschichten hinter den Kulissen.

Zeitverlust: Viele Nutzer merken gar nicht, wie viel Zeit sie täglich mit Shorts verbringen. Fünf Minuten hier, zehn da – und zack, ist ein ganzer Abend weg.

Abhängigkeit: Das Verhalten ähnelt in seiner Struktur einer Sucht. Man will „nur kurz" schauen, wird aber ständig getriggert, weiterzuwischen.

Was kann man dagegen tun?

1. Sich der Mechanismen bewusst werden

Nur wer weiß, wie die Algorithmen funktionieren, kann sich ihnen entziehen.

Wenn du weißt, dass die nächste Empfehlung nur deshalb kommt, weil du 5 Sekunden länger hingeschaut hast – bist du weniger verführbar.

2. Limit setzen

- Bildschirmzeit einschränken (z. B. mit Apps wie „Digital Wellbeing" oder „Screen Time")
- Pausen einbauen – oder gezielt Zeiten festlegen („Nur 10 Minuten Shorts pro Tag")

3. Andere Inhalte konsumieren

- Bewusst längere Videos anschauen
- Mal wieder einen Podcast hören
- Oder: ein gutes, altmodisches Buch lesen (ja, mit Seiten aus Papier)

4. Themenvielfalt fördern

- Gelegentlich bewusst Inhalte aus anderen Bereichen anschauen
- Kanäle abonnieren, die nicht deinem Alltag entsprechen

Fazit - Unterhaltung ja – aber mit Maß und Verstand
YouTube Shorts, Facebook Reels, TikTok – sie sind unterhaltsam, kreativ und manchmal sogar informativ. Aber sie sind eben auch designt, dich möglichst lange zu fesseln.

Die Plattformen verdienen Geld mit deiner Zeit – also sorgen sie dafür, dass du möglichst viel davon bei ihnen verbringst.

Wenn du dir dessen bewusst bist, kannst du bewusst entscheiden:
Bin ich heute in der Stimmung für etwas Kurzes und Schnelles – oder gönne ich mir echten Inhalt mit Tiefe?

Denn letztlich gilt:
Das nächste Video ist vielleicht gut – aber dein echtes Leben ist meistens besser.

Empfehlenswerte Quellen

Wikipedia: YouTube Shorts
https://en.wikipedia.org/wiki/YouTube_Shorts

Wikipedia: TikTok
https://de.wikipedia.org/wiki/TikTok

BSI: Online-Sucht
https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/o/online-sucht.html

Was machen TikTok & Co mit unserem Gehirn?
https://scilogs.spektrum.de/hirn-und-weg/was-machen-tiktok-co-mit-unserem-gehirn/

Kurz vergnügt - jetzt auch auf Youtube
https://www.sueddeutsche.de/medien/youtube-shorts-tiktok-1.5464790

Why is Social Media Addictive?
https://www.motleyrice.com/social-media-lawsuits/addiction

Willkommen in der Filterblase

Wie soziale Medien uns langsam einpacken

Stellen wir uns vor, soziale Medien wären ein gigantisches Einkaufszentrum. Am Anfang schlendern wir neugierig herum: ein bisschen Nachrichten hier, ein lustiges Katzenvideo dort, vielleicht noch ein Rezept für vegane Bananenbrot-Pizza. Alles schön bunt gemischt. Doch kaum haben wir uns ein zweites Mal ein Rezept angesehen, stürzt sich ein unsichtbarer Verkäufer auf uns – nennen wir ihn "Algorithmus" – und ruft begeistert: „Aha! Bananenbrot-Fan! Schnell, alles wegräumen, was nicht nach Banane riecht!“

Wie Algorithmen unsere Vorlieben ausspionieren

Algorithmen sind schlauer als der aufgeweckteste Marktschreier. Sie beobachten jedes Zögern, jedes Scrollen, jeden Klick. Sie notieren: „Benutzer hat Video über UFO-Sichtungen 7 Sekunden länger angesehen als Video über Steuerreform – UFOs wichtiger als Steuern.“ Und schon wird der ganze digitale Einkaufskorb vollgestopft mit fliegenden Untertassen, Kornkreisen und verschwörerischen Kornflakes.

Dabei geht es eigentlich nur um eines: Aufmerksamkeit. Die Plattformen wollen uns so lange wie möglich bei Laune – und auf der Seite – halten. Denn je mehr wir konsumieren, desto mehr Werbung kann uns untergeschoben werden. Und wie fesselt man Menschen am besten? Indem man ihnen genau das zeigt, was sie sowieso schon mögen oder spannend finden. Willkommen in der personalisierten Kuschelzone.

Der Weg in die Blase: Eine Einbahnstraße

Je öfter wir mit bestimmten Inhalten interagieren, desto mehr wird uns davon präsentiert. Anfangs ist das ganz angenehm: „Wow, der Algorithmus kennt mich besser als meine Mutter!“ Aber irgendwann wird's unheimlich: „Warum sehe ich nur noch vegane Kornkreisrezepte und keine echten Nachrichten mehr?“

Was passiert? Unsere Informationswelt wird kleiner. Widersprüchliche Meinungen? Andere Perspektiven? Fehlanzeige. Stattdessen entsteht eine virtuelle Echokammer, in der immer wieder die eigenen Ansichten reflektiert werden – nur eben lauter und schriller.

Und plötzlich sind Fake News die neuen Fakten

Wenn wir uns ständig in derselben Blase bewegen, erscheinen uns die präsentierten Inhalte immer glaubwürdiger. Schließlich sagen ja alle in unserem Newsfeed, dass die Erde eine Scheibe ist oder dass Einhörner eigentlich vom Mars stammen.

Unser Gehirn liebt Bestätigung – das nennt sich Bestätigungsfehler. Und soziale Medien servieren uns dieses Bestätigungsmenu auf einem goldenen Tablett, inklusive Gratisnachschlag. Kritisches Denken? Wird schwierig, wenn man von 37 Likes und 12 Kommentaren Bestätigung bekommt: „Ja, du hast recht, Mars-Einhörner sind real!“

Und was nun?

Ganz ehrlich: Komplett entkommen können wir den Algorithmen kaum – es sei denn, wir ziehen in eine Hütte im Wald ohne WLAN. Aber wir können wachsam bleiben: bewusst verschiedene Quellen lesen, aktiv nach anderen Meinungen suchen und immer wieder den inneren Alarm schrillen lassen, wenn etwas zu schön klingt, um wahr zu sein.

Denn eines ist sicher: Wer nur noch das sieht, was er sowieso schon glaubt, wird irgendwann glauben, dass Bananenbrot die Antwort auf alle Fragen ist.

Und seien wir ehrlich – so lecker ist Bananenbrot nun auch wieder nicht.

Empfehlenswerte Quellen (Bücher / Studien)

Diese Studien kann man über eine WebSuche finden...

Bakshy et al. (2015) – Exposure to ideologically diverse news and opinion on Facebook (Science-Studie)

Nickerson (1998) – Confirmation Bias: A Ubiquitous Phenomenon in Many Guises

Vosoughi, Roy & Aral (2018) – The spread of true and false news online (Science-Studie über Fake News)

Cass Sunstein – #Republic: Divided Democracy in the Age of Social Media (Buch über Echokammern)

Cathy O'Neil – Weapons of Math Destruction (Buch über die Gefahren von Algorithmen)

Hilfe, mein Akku ist schon wieder leer!

Warum Smartphones ständig nach der Steckdose rufen

Achtung... Mal ein längeres Kapitel!

Montagmorgen, 8 Uhr: Dein Smartphone zeigt 100 % Akkuladung. 11 Uhr: noch 37 %. Kommt dir bekannt vor? Moderne Handys entwickeln manchmal einen erstaunlichen Durst – der Akku scheint schneller schlapp zu machen als man „Ladekabel" sagen kann. Woran liegt's, und was kann man tun? In diesem humorvoll-sachlichen Ratgeber werfen wir einen Blick auf die üblichen Verdächtigen beim raschen Akkuverbrauch und zeigen, wie du den kleinen Energieräubern den Stecker ziehst (zumindest sprichwörtlich).

Technische und alltägliche Gründe: Der Akku ruckzuck leer ist...

Eines vorweg: Der größte Akkufresser ist das Display. Ein hell beleuchteter Bildschirm zieht enorm viel Strom . Logisch – schließlich leuchten heute riesige, hochauflösende Anzeigen in unseren Hosentaschen. Wer die Displayhelligkeit reduziert, kann also direkt einiges an Akku sparen . Besonders OLED- oder AMOLED-Bildschirme profitieren vom Dunkelmodus: Hier werden dunkle Bildpunkte einfach gar nicht beleuchtet und verbrauchen somit praktisch keine Energie . Laut einer Google-Untersuchung ließ sich der Energieverbrauch bei maximaler Helligkeit im Dark Mode um 63 % reduzieren (im Vergleich zum hellen Modus) – wow! Kein Wunder, dass der Dark Mode inzwischen überall im Einsatz ist. Und falls dein Handy ein schickes Always-On-Display hat, das ständig Uhrzeit und Benachrichtigungen zeigt, überlege dir, ob du es wirklich brauchst – auch ein teildeaktiviertes Display nuckelt am Akku und mindert die Laufzeit .

Neben dem Bildschirm kann auch die Verbindungstechnik deinen Akku an den Rand der Erschöpfung treiben. Allen voran 5G: Der neue Mobilfunk-Turbo bringt irre Downloadraten, gönnt sich dabei aber gerne einen kräftigen Schluck aus dem Akku-Becher. In der Praxis zeigt sich nämlich, dass 5G-Verbindungen derzeit oft mehr Energie ziehen als 4G/LTE . Bei ersten 5G-Smartphones wie dem Galaxy S20 führte 5G teils dazu, dass der Akku bis zu 60 % schneller leer war als im 4G-Betrieb . Ursache ist meist der Non-Standalone-Betrieb: Das Handy funkt gleichzeitig in 4G und 5G, was doppelt am Akku zehrt . Ähnlich anstrengend ist permanenter Funkstress durch schlechten Empfang. Wenn du dich im Funkloch oder einem Gebäude mit Stahlbeton befindest, bemüht sich das Telefon verzweifelt um ein Signal – und verbraucht dabei reichlich Energie. GPS und Ortungsdienste sind ein weiterer stiller Akku-Killer: Sobald die Standortfunktion aktiv ist, lauscht der GPS-Chip kontinuierlich nach Satelliten. Das Handy kann dann gar nicht in den Schlafmodus gehen, weil ständig die Position aktualisiert wird . Insbesondere Navigations-Apps oder Standort-Tracking sorgen dafür, dass dein Smartphone wach bleibt und fleißig Strom zieht. Eine aktuelle Studie zeigte, dass eine GPS-App in nur kurzer Zeit 13 % der Akkukapazität verbrauchte – bei gutem Signal. In einem Gebiet mit schlechtem Empfang schoss der Verbrauch sogar auf 38 % hoch . Kurz gesagt: Wenn das Handy permanent „Wo sind wir?“-Ping spielt, schmilzt der Akku dahin.

Auch Hintergrunddienste und -apps tragen zum Akkuhunger bei. Selbst wenn du das Telefon gerade nicht aktiv nutzt, werkeln im Hintergrund oft Dutzende Prozesse: E-Mails werden synchronisiert, Widgets aktualisieren das Wetter, Chat-Apps horchen auf neue Nachrichten, und so weiter. Je mehr ungenutzte Apps im Hintergrund laufen, desto mehr Energie verbraucht der Akku – so einfach ist das. Viele Systeme haben zwar Mechanismen, um Hintergrundverbrauch zu zügeln, aber Wunder darf man nicht erwarten. Sogar Sprachassistenten können überraschend viel Strom ziehen: Google Assistant etwa horcht

ständig auf sein „OK Google“-Kommando und benötigt dafür dauerhaft etwas Mikrofon- und Rechenpower . Klingt nach wenig, summiert sich aber über den Tag. Und natürlich gilt: Ist der Akku selbst nicht mehr der fitteste (Stichwort Alterung nach ein bis zwei Jahren), geht ihm ohnehin schneller die Puste aus – doch das ist ein Thema für sich.

Apps als Akkufresser: Social Media, Spiele & Navigation

Im Alltag entleeren nicht nur Technik-Komponenten den Akku, sondern vor allem unsere liebsten Apps. Manche Anwendungen sind so energiehungrig, dass man ihnen am liebsten ein eigenes Ladegerät spendieren würde. Allen voran stehen Social-Media-Apps. Ob Instagram, Facebook, TikTok oder WhatsApp – sie alle fordern den Akku gleich doppelt: Einerseits durch ständige Online-Verbindung und datenintensive Inhalte (hallo, Auto-Play-Videos und endloses Scrollen), andererseits durch Hintergrundaktivitäten wie Synchronisierung und Push-Benachrichtigungen. Untersuchungen belegen, dass diverse Social-Apps zu den Top-Akkukillern gehören. Laut einer Analyse von pCloud (2023) stellen soziale Netzwerke 6 der 20 energieintensivsten Apps, da sie durchschnittlich 11 zusätzliche Funktionen im Hintergrund aktivieren (von Standort über Mikrofon bis WLAN) . Mehr Hintergrund-Action bedeutet mehr Stromhunger – dein Akku führt quasi ein Eigenleben, selbst wenn du die App gerade geschlossen hast. Und ja, auch Video-Streaming à la YouTube oder Netflix hat einen ähnlichen Effekt: Permanentes Abspielen von Medien bei aktiviertem Display lässt die Prozentanzeige rapide sinken .

Dicht gefolgt im Akku-Ranking sind Mobile Games. Klar, Zocken macht Spaß – aber auf Smartphones kann es den Akku so schnell leersaugen wie ein 3D-Grafikvampir. Spiele fordern Prozessor und Grafikchip maximal, wärmen das Gerät (ein sicheres Zeichen, dass Energie in Hitze verpufft) und halten das Display permanent an. Viele aktuelle Games laufen mit hohen Bildraten und knalligen Effekten, was

dazu führen kann, dass dein Handy schon nach ein paar Stunden Spielzeit schlappmacht. Wenn du also mal wieder unterwegs einen „Boss-Gegner“ erledigst und dich wunderst, warum dein Telefon sich fast so anfühlt wie eine heiße Tasse Kaffee: Das ist dein Akku, der Schwerstarbeit leistet. Immerhin gönnen einige Spiele deinem Gerät keine Pause – da wird gerechnet, funkt eventuell online (für Multiplayer oder Cloud-Speicherstände) und natürlich nonstop hell angezeigt. Kurzum: Mobile Games sind der Sprintlauf für deinen Akku, Marathonlaufen liegt ihm eigentlich mehr.

Ein weiterer großer Posten auf der Akkuverbrauchs-Liste: Navigations- und Tracking-Apps. Jeder, der schon einmal mit Google Maps, Apple Karten oder Waze länger unterwegs war, kennt das Phänomen: Trotz voller Ladung am Start steht das Akku-Level nach einer längeren Fahrt oder Wanderung bedenklich niedrig. Navigation kombiniert die härtesten Disziplinen für den Akku: dauerhaftes GPS, mobile Daten, kontinuierende Neuberechnung von Routen und ein eingeschaltetes Display (oft auf hoher Helligkeit, damit man die Karte auch in der Sonne erkennt). Da überrascht es nicht, dass Navigation zu den schnellsten Wegen gehört, einen Akku in die Knie zu zwingen. In einem Tech-Test hielt ein Smartphone bei eingeschaltetem GPS und Navigations-App teils nur rund 2 Stunden durch – dann war Schluss (je nach Modell kann das variieren). Selbst Mitfahr- und Liefer-Apps wie Uber oder Lieferdienste nagen am Akku, weil sie ständig deinen Standort verfolgen. Fun-Fact am Rande: Laut der bereits erwähnten pCloud-Analyse zählen auch Dating-Apps zu den heimlichen Stromräubern – etwa 15 % der Top-Akkufresser waren Tinder & Co., die nicht nur Herzklopfen, sondern auch hohe Hintergrundaktivität (durchschnittlich 11 laufende Ressourcen) verursachen und oft keinen Dark Mode bieten . Die Liebe mag blind sein, aber der Akku merkt’s trotzdem.

Aktuelle Tipps und Tricks: So hält dein Akku länger durch

Keine Panik – du musst jetzt nicht alle Lieblingsapps löschen oder das Smartphone nur noch im „Museumsmodus“ betreiben. Mit ein paar praktischen Akkuschon-Tipps lässt sich viel erreichen, ohne den Spaß am Gerät zu verlieren. Hier kommen konkrete, aktuelle Strategien, mit denen dein Akku nicht mehr ganz so schnell die Grätsche macht.

Display dimmen & Dark Mode nutzen: Reduziere die Bildschirmhelligkeit auf ein angenehmes Maß, anstatt ständig auf 100 % zu leuchten. Stell außerdem überall den Dark Mode ein, wo es geht – sowohl im System als auch in beliebten Apps (viele bieten diese Option inzwischen an, z. B. WhatsApp) . Besonders auf OLED-Displays bringt das was, denn Schwarz benötigt dort quasi keinen Strom . Deine Augen freuen sich obendrein über weniger grelles Licht. Auch hilfreich: Bildschirm-Timeout kurz halten. Lass das Display z. B. nach 30 Sekunden Inaktivität ausgehen statt nach mehreren Minuten . Jede Sekunde weniger An-Zeit spart Strom. Und wenn du kein Always-On-Display brauchst, deaktiviere es – der Akku wird es dir danken .

Datenverbindungen gezielt kappen: Schalte Verbindungen aus, die du gerade nicht nutzt . Beispielsweise NFC aus, wenn du nicht via Handy zahlst. Bist du sowieso daheim oder im Büro im WLAN, kannst du getrost die mobile Datennutzung deaktivieren – dein Handy funkt dann nicht dauernd im Mobilnetz herum . Gleiches gilt für Bluetooth (aus damit, wenn keine Kopfhörer oder Smartwatch verbunden sind) und GPS, wenn du es nicht aktiv brauchst . Selbst 5G kannst du bei Akkunot zur Not temporär auf 4G umstellen – insbesondere in Regionen mit schlechtem 5G-Empfang, wo das ständige Netzwechseln viel Energie frisst . Kurz gesagt: Alles, was nicht gebraucht wird, in den Flugmodus schicken (oder gezielt abschalten). Dein Telefon muss nicht permanent auf jeder Party mittanzen.

Hintergrundaktivität einschränken: Viele kleine Apps summieren sich zu einem großen Durst. Geh in die Einstellungen und überprüfe, welche Anwendungen im Hintergrund aktiv sind. Schließe Apps, die du nicht benutzt, und erlaube nicht jeder App, dauernd im Hintergrund zu laufen. Moderne Smartphones bieten oft Funktionen, um Apps automatisch schlafen zu legen, wenn sie lange ungenutzt sind . Nutz diese Features! Denn je mehr unnötige Apps im Hintergrund werkeln, desto schneller ist der Akku leer . Überlege auch, unnötige Konten oder Synchronisierungen zu entfernen – jedes verknüpfte Konto (sei es ein Zweit-E-Mail-Postfach oder eine längst vergessene App-Verbindung) synchronisiert sonst fleißig Daten im Hintergrund . Ähnliches gilt für Push-Benachrichtigungen: Schalte Mitteilungen für Apps ab, die dich nicht ständig informieren müssen . Dein Handy checkt dann seltener neue Updates und spart Strom – und du sparst Nerven . Auf iPhones kann man etwa die Hintergrundaktualisierung für bestimmte Apps deaktivieren, was direkt etwas Akkulaufzeit herauskitzelt .

Energiesparmodus und Optimierungen nutzen: Sowohl Android als auch iOS haben eingebaute Energiesparmodi. Diese Modi drosseln z. B. die Prozessorleistung, reduzieren visuelle Effekte und beschränken Hintergrunddienste – und können so die Akkulaufzeit deutlich verlängern . Keine Sorge, dein Smartphone wird dadurch nicht unbenutzbar, es ist eher so, als würde es in den Ruhemodus schalten, wenn maximale Performance gerade nicht nötig ist. Probier's ruhig aus, vor allem wenn dein Akkustand kritisch wird. Viele Geräte haben auch intelligente Gerätewartung-Funktionen: Einmal auf „Jetzt optimieren“ tippen, schon werden unnötige Hintergrund-Apps geschlossen und Stromfresser gebremst . Mach dich in den Einstellungen schlau, was dein Handy hier anbietet. Und last but not least: Halte dein Betriebssystem und Apps aktuell. Oft bringen Updates Fehlerbehebungen, die Bugs wie übermäßigen Akkuverbrauch

eliminieren . Wenn eine bestimmte App plötzlich viel Akku zieht, könnte ein Update oder notfalls eine Neuinstallation Wunder wirken .

Sonstige Stellschrauben: Es gibt noch ein paar kleinere Tricks, die in Summe helfen. Zum Beispiel kannst du die Vibrationsfeedbacks ausschalten (jede kleine Vibration kostet etwas Strom) , den Ton bei Tastendruck deaktivieren und lieber auf visuelle Benachrichtigungen setzen statt auf dauerndes vibrieren oder Klingeln – der lautlose Modus ist am sparsamsten . Auch Widgets, die sich ständig aktualisieren (z. B. Live-Wetter auf dem Homescreen), zerren am Akku . Reduziere solche Live-Widgets auf das Nötigste. Und wenn's ganz eng wird: In kritischen Situationen hilft der Flugmodus (schaltet alle Funkverbindungen ab) oder zur Not das komplette Abschalten nicht benötigter Features, bis du die nächste Steckdose erreichst.

Fazit - Der Smartphone-Akku wird im Alltag von vielen Seiten in die Mangel genommen: Ein helles Display, ständig aktive Funkmodule (5G, GPS & Co) und energieintensive Apps saugen gemeinsam an der Batteriezelle. Social-Media-Apps, Spiele und Navigation gehören dabei zu den größten Stromfressern, die teils unbemerkt im Hintergrund werkeln und am Akkustand nagen. Die gute Nachricht: Mit ein paar cleveren Einstellungen – von Display-Dimmung über Dark Mode bis Energiesparmodus – lässt sich die Laufzeit deutlich verbessern, ohne dass du dein Nutzungsverhalten komplett auf den Kopf stellen musst. Und solltest du doch mal mit leerem Akku dastehen, denk dran: Du bist nicht allein – und vielleicht liest du das nächste Mal diesen Artikel, bevor der Akku rot blinkt.

Empfehlenswerte Quellen

Smartphone-Akku schnell leer? Eine praktische Funktion kann helfen
https://www.techbook.de/mobile-lifestyle/smartphone/apps-android-akku-verbrauch-fressen

Ist 5G beim Smartphone ein Akkufresser?
https://www.4g.de/news/ist-5g-smartphone-akkufresser-12460/

Android: Handy-Akku schnell leer - daran kann es liegen!
https://www.techbone.de/android/handy-akku-schnell-leer

Handy-Akku schnell leer: Häufige Ursachen und Lösungen
https://www.chip.de/news/Handy-Akku-schnell-leer-Haeufige-Ursachen-und-Loesungen_185321074.html

inside digital – Akku-Tricks 2025: So hält dein Handy länger durch:
https://www.futurezone.de/digital-life/verbraucher/article401358/sechs-tricks-handy-deaktivierung-schnelligkeit.html

Handy-Trick: Sofort bessere Leistung – klappt bei jedem Modell
https://www.futurezone.de/digital-life/article502100/handy-trick-akku-verlaengern.html

Künstliche Intelligenz

oder wie wir das Denken abgeben

Vom Kopf ins Kabel: Eine Einleitung

Früher war Denken harte Arbeit. Heute ist es vor allem eines: ausgelagert. An Algorithmen, Apps, smarte Assistenten und all die digitalen Helferlein, die unser Leben effizienter – und unser Hirn gelegentlich überflüssig – machen.

Ob es um die Wahl des nächsten Films, den besten Weg zur Tankstelle oder um den Partner fürs Leben geht – Künstliche Intelligenz (KI) weiß oft schon, was wir wollen, bevor wir überhaupt anfangen zu denken. Und wir? Sagen artig „Danke, Alexa" und wundern uns, warum wir unseren PIN nicht mehr auswendig wissen.

Aber wie konnte es so weit kommen? Wie wurde aus einem einfachen Schachcomputer ein Chatbot, der Hausarbeiten schreibt? Und was macht das eigentlich mit uns – gesellschaftlich, geistig, menschlich?

Die ersten Schritte: Schach, Psychotherapie und bitweise Begeisterung

Die Reise beginnt in den 1950er Jahren. Damals träumten Forscher davon, Maschinen zu bauen, die „denken" können – was immer das auch genau heißen sollte. Erste Programme wie ELIZA simulierten Gespräche mit einem Therapeuten, indem sie die Sätze des Nutzers in höfliche Fragen zurückwarfen. Eine Art digitaler Papagei mit Doktortitel. Überraschend viele Menschen hielten das damals schon für echte

Intelligenz – was viel über Menschen aussagt und wenig über Maschinen.

Dann kam der große Moment: 1997 schlug Deep Blue, ein Supercomputer von IBM, den amtierenden Schachweltmeister Garri Kasparow. Kein Zufall, sondern Rechenpower auf Steroiden. Der Computer konnte keine Emotionen, keine Intuition – aber eben 200 Millionen Stellungen pro Sekunde durchrechnen. Das genügte. Und der Mensch hatte erstmals offiziell verloren.

Lernen statt Regeln: Wenn Maschinen sich selbst verbessern

Nach Deep Blue wurde klar: Regeln reichen nicht aus. Maschinen mussten lernen, nicht nur befolgen. Willkommen im Zeitalter des Maschinellen Lernens.

Statt mühsam alles zu programmieren, gibt man der KI große Datenmengen – und sie findet selbst heraus, wie man z. B. eine Katze erkennt, Texte übersetzt oder das Go-Spiel dominiert. Der Durchbruch kam 2016, als AlphaGo einen der besten Go-Spieler der Welt besiegte. Dieses Spiel war so komplex, dass es lange als zu schwierig für Computer galt.

Der Trick: Deep Learning, also künstliche neuronale Netze mit vielen „Schichten" – wie ein digitales Gehirn mit ganz viel Kaffee. Die Maschine spielte Millionen Partien gegen sich selbst, lernte aus Fehlern und wurde besser als jeder Mensch. Ohne Bauchgefühl, aber mit beeindruckender Statistik.

Die KI zieht ein: Alltag, Auto, Arztpraxis

Heute ist KI nicht mehr in Supercomputern eingesperrt. Sie wohnt in deinem Smartphone, deinem Fernseher, deinem Auto – manchmal sogar in deiner Zahnbürste.

ChatGPT & Co.

Große Sprachmodelle wie ChatGPT schreiben Aufsätze, Liebesbriefe und Bewerbungen. Sie texten besser als viele Menschen – oder zumindest schneller. Möglich macht das ein Training mit Milliarden Sätzen aus dem Internet. Und ja, auch dieser Text könnte theoretisch von einer KI stammen. Wer weiß?

Autonomes Fahren

Autos, die alleine fahren? Noch nicht ganz serienreif, aber ziemlich nah dran. Unternehmen wie Tesla oder Waymo testen selbstfahrende Fahrzeuge auf öffentlichen Straßen. Der Mensch wird vom Fahrer zum Passagier – und darf sich schon mal überlegen, wo er künftig noch das Steuer übernehmen darf.

Medizin

KI kann heute Hautkrebs besser erkennen als viele Dermatologen, Tumore auf Röntgenbildern finden und in Sekundenschnelle Therapievorschläge machen. Natürlich ersetzt sie keine Ärztin – aber sie unterstützt. Und sie vergisst keine Details, ist nie müde und googelt nicht während der OP.

Streaming & Shopping

Netflix, Amazon, Spotify – alle nutzen KI, um dir genau das zu zeigen, was du vermutlich eh schon willst. Bequem? Ja. Aber vielleicht bekommst du so nie mit, dass du eigentlich Jazz mögen würdest. Willkommen in der Filterblase.

Komfort mit Nebenwirkungen

Künstliche Intelligenz macht das Leben bequemer. Aber Bequemlichkeit hat ihren Preis. Je mehr Entscheidungen wir Maschinen überlassen, desto weniger üben wir das Entscheiden.

Psychologen sprechen vom kognitiven Outsourcing. Wir verlernen, Fakten zu prüfen, abzuwägen, selbst zu denken – weil es einfach ist, der Empfehlung zu folgen. Warum sich mit komplexen Meinungen beschäftigen, wenn der Algorithmus schon entschieden hat, was „gut für dich“ ist?

Und dann ist da noch das Thema Manipulation: Wenn eine KI weiß, was du sehen willst – was hindert sie daran, dir zu zeigen, was du sehen sollst? Fake News, Deepfakes, personalisierte Werbung – all das nutzt KI, um Einfluss zu nehmen. Und das oft, ohne dass du es merkst.

Blick in die Zukunft: Zwischen Butler und Big Brother

Wie sieht die Zukunft aus? Im besten Fall: KI erledigt langweilige Jobs, wir Menschen konzentrieren uns auf Kreativität, Beziehung, Sinn. Im schlimmsten Fall: Maschinen übernehmen Entscheidungen, Arbeitsplätze und irgendwann vielleicht sogar die Kontrolle.

Einige warnen vor der sogenannten Superintelligenz – einer KI, die schlauer ist als der Mensch in jeder Hinsicht. Andere glauben an die „freundliche KI“, die uns dient, nicht dominiert. Fakt ist: Die Weichen stellen wir. Jetzt.

Fazit - Denken abgeben? Mit Maß und Ziel! Künstliche Intelligenz ist faszinierend. Sie kann uns entlasten, inspirieren, sogar retten. Aber sie darf uns nicht das Denken abgewöhnen.

Nutzen wir sie als Werkzeug – nicht als Ersatz für unseren Verstand. Denn am Ende gilt: Nur wer selbst denkt, kann entscheiden, was richtig ist. Und wer nur klickt, was vorgeschlagen wird, lebt vielleicht bequem – aber nicht frei.

Empfehlenswerte Quellen

Wikipedia – Künstliche Intelligenz
https://de.wikipedia.org/wiki/K%C3%BCnstliche_Intelligenz

Stanford AI Index 2024
https://hai.stanford.edu/ai-index/2024-ai-index-report

OpenAI – Einführung ChatGPT
https://openai.com/de-DE/chatgpt/overview/

IBM Deep Blue Projekt
https://www.ibm.com/history/deep-blue

BSI – Deepfakes und Sicherheit
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

Deutschlandfunk Kultur – 50 Jahre ELIZA
https://www.deutschlandfunkkultur.de/50-jahre-software-eliza-vom-psychiater-inspirierte-100.html

Bitcoin

Warum ein paar Nullen und Einsen plötzlich mehr wert sind als dein Auto – und wer sich darüber ganz besonders freut.

Die Geburt des Bitcoin – und niemand kam mit Luftschlangen

Im Januar 2009 wurde der erste Block der Bitcoin-Blockchain geschürft – der sogenannte Genesis-Block. Verantwortlich dafür: ein bis heute unbekannter Mensch (oder eine Gruppe?) namens Satoshi Nakamoto. Der Name klingt wie ein japanischer Hacker aus einem Cyberpunk-Film – und das passt auch irgendwie.

In einer Welt, die gerade mit der Finanzkrise kämpfte, hatte Nakamoto einen radikalen Vorschlag: Was wäre, wenn man Geld digitalisiert, völlig dezentralisiert und ohne Banken dazwischenschaltet? Die Idee: Jeder kann mitmachen, niemand hat die Kontrolle allein, und das System regelt sich selbst – dank Mathematik, Kryptografie und einer eleganten Datenstruktur namens Blockchain.

Warum ist ein Bitcoin so teuer?

Anfangs konntest du für ein paar Cents gleich mehrere Bitcoins kaufen. Der erste dokumentierte Kauf eines physischen Produkts mit Bitcoin war übrigens eine Pizza – für 10.000 BTC. Heute wäre das die wohl teuerste Pizza der Menschheitsgeschichte (circa 960 Millionen Euro bei einem Kurs von etwa 96.000 €/BTC, Stand: Mai 2025).

Aber warum dieser Wertanstieg?

Begrenztes Angebot: Es wird niemals mehr als 21 Millionen Bitcoins geben. Diese Knappheit erinnert an Gold – und deshalb spricht man auch vom digitalen Gold.

Nachfrage-Boom: Immer mehr Menschen, Unternehmen und sogar Länder springen auf den Bitcoin-Zug auf – als Absicherung gegen Inflation, als Spekulationsobjekt oder einfach, weil's hip ist.

Mediale Aufmerksamkeit: Je mehr darüber berichtet wird, desto mehr Menschen investieren – was den Preis weiter antreibt (und dann... wieder abstürzen lässt, siehe nächster Punkt).

Volatilität – Wenn dein Bitcoin-Portemonnaie Achterbahn fährt

Bitcoin ist wie ein hyperaktiver Teenager auf Zucker – es kann binnen Minuten in den Himmel schießen und genauso schnell wieder zusammenbrechen. Gründe dafür sind:

- Spekulation durch Großanleger
- Regulierungsnachrichten
- Tweets von Elon Musk (ja, wirklich)
- Gerüchte, Hackerangriffe, Stromausfälle in Mining-Zentren

Für Investoren heißt das: Wer keine starken Nerven hat, sollte besser bei klassischen Sparkonten bleiben (auch wenn die 0,5 % Zinsen eher wie ein feuchter Händedruck wirken).

Mining – digitale Schürfarbeit mit echtem Stromhunger

Mining ist der Prozess, bei dem neue Bitcoins entstehen und Transaktionen verifiziert werden. Dabei lösen spezialisierte Computer weltweit extrem komplexe Rechenaufgaben – sogenannte Hash-Funktionen. Der erste, der die Lösung findet, bekommt eine Belohnung in Form von neuen Bitcoins.

Aber: Dieser digitale Schatzsucher-Prozess braucht enorm viel Strom. Und zwar so viel, dass das Bitcoin-Netzwerk inzwischen mehr Energie verbraucht als ganze Länder – etwa Polen, Argentinien oder die Niederlande.

Warum ist das so?

Der Rechenaufwand ist gewollt schwierig, um das System sicher zu machen. Wer schneller rechnet, hat mehr Chancen – also wird aufgerüstet.

Und wer Strom billig bekommt (siehe nächster Punkt), hat einen Vorteil.

Warum „Schurkenstaaten" Mining lieben

Für Staaten wie Iran, Nordkorea oder Venezuela, die wirtschaftlich unter Sanktionen leiden, ist Bitcoin-Mining eine clevere Methode, um an internationale Devisen zu kommen – ohne dass westliche Banken oder Behörden dazwischenfunken können.

Was sie so attraktiv finden:

- Strom ist oft staatlich subventioniert.
- Die Coins können anonym verkauft werden.
- Es gibt keine zentrale Kontrollinstanz, die einen rausschmeißen kann.
- Mining-Hardware ist oft über Umwege zu bekommen – und dann geht's los.
- So wird aus einer alten Textilfabrik ein Bitcoin-Mining-Zentrum – mit brummenden Grafikkarten, glühenden Netzteilen und einem Außenminister, der sagt: "Wir haben den digitalen Kapitalismus endlich verstanden."

Risiken: Wenn dein Wallet das Zeitliche segnet

Der Reiz von Bitcoin liegt in der Dezentralisierung – aber genau das ist auch das Risiko:

- **Verlorene Schlüssel** = verloren für immer. Niemand kann dein Passwort zurücksetzen. Kein "Passwort vergessen"-Link. Nur du und deine Verantwortung.
- **Keine Rückbuchungen.** Wenn du versehentlich 5 BTC an die falsche Adresse schickst, kannst du höchstens hoffen, dass der Empfänger ein ehrlicher Mensch ist – was in der Finanzwelt etwa so wahrscheinlich ist wie ein freundlicher Troll.
- **Hackbare Börsen.** Zwar ist die Blockchain an sich ziemlich sicher – aber die Plattformen, auf denen du deine Bitcoins kaufst oder lagerst, wurden in der Vergangenheit immer wieder Opfer spektakulärer Hacks.

Fazit- Der Bitcoin ist kein Teufel – aber auch kein Heilsbringer! Bitcoin ist ein faszinierendes technologisches Experiment – mit dem Potenzial, das traditionelle Finanzsystem herauszufordern. Er steht für Freiheit, Dezentralisierung und eine neue Form der Unabhängigkeit. Doch er bringt auch ökologische, wirtschaftliche und sicherheitstechnische Probleme mit sich.

Wer in Bitcoin investieren will, sollte nicht nur an schnelles Geld denken, sondern auch bereit sein, das System zu verstehen – und Risiken zu tragen. Denn wie beim Goldrausch im Wilden Westen gilt auch hier: Nicht jeder wird reich. Aber viele verkaufen immerhin Schaufeln. Oder heute: Grafikkarten.

Empfehlenswerte Quellen

Wikipedia: Bitcoin
https://de.wikipedia.org/wiki/Bitcoin

Finanzen.net: Warum die Sparkassen für 2025 weiter von Investments in Bitcoin abraten
https://www.finanzen.net/nachricht/devisen/trotz-kryptorally-warum-die-sparkassen-fuer-2025-weiter-von-investments-in-bitcoin-abraten-14071355

Zum Abschluss

Du hast es bis hierher geschafft – und dafür erst einmal: Danke!

In diesem kleinen Buch haben wir gemeinsam hinter die glänzende Oberfläche deines Smartphones geschaut. Wir sind durch die Geschichte des Telefons gereist, haben die Technik unter der Haube kennengelernt, uns mit Prozessoren, SIM-Karten, Betriebssystemen, WLAN, VPNs, Browsern und Passwörtern beschäftigt – und dabei immer wieder die Frage gestellt: Was weiß mein Smartphone eigentlich über mich? Und wie kann ich mich (und meine Daten) besser schützen?

Ob du nun neugieriger geworden bist, ein paar Einstellungen angepasst hast oder einfach nur ein besseres Gefühl dafür hast, was in deiner Hosentasche jeden Tag mitläuft – dieses Buch hat hoffentlich dazu beigetragen, dass du dich in der digitalen Welt ein bisschen sicherer und bewusster bewegst.

Danke, dass du dir die Zeit genommen hast, dieses Buch zu lesen. Bleib smart – aber nicht smart dumm.

Bonus: Was ist eine Paywall

und wie frei sind Nachrichten im Internet wirklich?

Das Internet galt lange als Ort des freien Zugangs zu Wissen und Informationen. Doch wer heute Nachrichten online lesen möchte, stößt oft auf eine Paywall – eine digitale Bezahlschranke, die Inhalte nur nach Zahlung zugänglich macht. Doch was genau ist eine Paywall, warum gibt es sie – und bedeutet das, dass Nachrichten heute nicht mehr „frei“ sind?

Was ist eine Paywall?

Der Begriff Paywall setzt sich aus den englischen Wörtern pay (bezahlen) und wall (Mauer) zusammen. Gemeint ist damit ein System auf Nachrichtenseiten oder Online-Medien, das den Zugriff auf Inhalte einschränkt. Wer den vollständigen Artikel lesen will, muss entweder ein Abonnement abschließen oder eine Einmalzahlung leisten.

Es gibt verschiedene Modelle:

- Harte Paywall: Ohne Bezahlung sieht man gar nichts.
- Weiche Paywall: Einige Artikel sind frei, der Rest kostenpflichtig.
- Metered Paywall: Man kann z. B. fünf Artikel im Monat kostenlos lesen, danach wird bezahlt.

Warum gibt es Paywalls?

Qualitätsjournalismus kostet Geld. Redakteurinnen und Redakteure, Reporter, Fotografen, Technik – all das muss finanziert werden. Früher geschah das über den Verkauf von Zeitungen und Anzeigen. Online-Werbung allein reicht heute oft nicht aus, um die journalistische Arbeit zu tragen. Daher setzen viele Medienhäuser auf Bezahlmodelle.

Sind Nachrichten dann noch „frei“?

Das ist eine berechtigte Frage – und eine umstrittene. Auf der einen Seite ist die Pressefreiheit dadurch nicht gefährdet: Medien dürfen weiterhin unabhängig berichten. Auf der anderen Seite entsteht eine soziale Hürde: Wer nicht zahlen kann oder will, bleibt außen vor.

Besonders heikel wird es, wenn wichtige Informationen – etwa zu Politik, Gesundheit oder gesellschaftlichen Entwicklungen – nur hinter der Paywall erscheinen. Dann stellt sich die Frage, ob ein zentraler Auftrag des Journalismus, nämlich die informierte Öffentlichkeit, noch erfüllt wird.

Ein neues Informationsgefälle?

Wenn Informationen nur noch gegen Geld zugänglich sind, entsteht ein digitales Ungleichgewicht: Wissen wird zum Luxus. Während einige Menschen Zugang zu fundierter Berichterstattung haben, bleiben andere auf Social Media, Schlagzeilen oder Halbwissen angewiesen. Das kann langfristig zu einer Spaltung der Gesellschaft führen.

Fazit - Paywalls sind aus Sicht der Medien wirtschaftlich notwendig – aber sie werfen grundlegende Fragen über den Zugang zu Informationen in einer Demokratie auf. Die Herausforderung besteht darin, ein Gleichgewicht zu finden: Journalismus fair finanzieren, ohne die Allgemeinheit vom Wissen auszuschließen. Denn nur informierte Menschen können sich eine fundierte Meinung bilden – und genau das ist das Fundament einer freien Gesellschaft.

Empfehlenswerte Quellen

Wikipedia: Paywalls
https://de.wikipedia.org/wiki/Paywall

SocialMedia One Paywall - Was ist das? Geld verdienen mit Views, Modelle, Rechenbeispiel
https://socialmediaone.de/paywall-was-ist-das-geld-verdienen-views-modelle-rechenbeispiel/

Heise: Was ist eine PayWall
https://www.heise-homepages.de/glossary/paywall/